UNIVERSIDAD POLITÉCNICA DE MADRID

FACULTAD DE INFORMÁTICA

# ESTUDIO COMPARATIVO DE PROTOCOLOS DE ENCAMINAMIENTO EN REDES VANET

Trabajo Fin De Carrera

AUTOR:HÉLÈNE DOUMENC
TUTOR:JOSE MARÍA PEÑA

JUNIO DE 2008

# Agradecimientos

No es fácil agradecer en pocas palabras a todas las personas que han hecho posible que se lleve a cabo este proyecto de fin de carrera. Pero todos los que no menciono se saben aludidos.

En primer lugar y en un plano personal quiero agradecer a mis padres todo los esfuerzos y sacrificios que han hecho para que pueda llegar ser la persona que soy hoy en día y para que pueda cumplir con mis ambiciones. También agradecerles a mis hermanos, Nicolas y Dalila, la comprehensión y el apoyo recibido a lo largo de todos esos años.

Es necesario mencionar a mis compañeros de universidad que son mis amigos y que me han acompañado todos esos años en los buenos y en los malos momentos. Doy las gracias a Benji, Rita, Rémi Allègre, Rémi Cazenave. Espero poder ayudaros como me habéis ayudado.

En un plan profesional quiero agradecer a mi tutor en Telefónica, Iván Lequerica Roca. Ha hecho posible la realización de este proyecto, me ha apoyado para que pueda integrarme en la empresa y gracias a sus consejos y directivas me ha enseñado mucho. No puedo olvidar tampoco a mis compañeros de trabajo que me han ayudado siempre que lo podían y que me han permitido trabajar en un ambiente agradable. Pienso en particular en Miguel que además de compañero es amigo.

En último lugar he de reconocer que he aprendido mucho de mis profesores en la universidad, tanto en Francia como en Espña. Gracias a M. Titli para ayudarme a cumplir mi deseo de obtener un doble título. Ha hecho posible que pueda estudiar España y en parte gracias a él estoy viviendo una de las experiencias más enriquecedora de mi vida. En Madrid, conocí a José María Peña que me ayudó en un momento crucial de cambio, siempre estuvo presente para resolver cualquier problema o duda. Es también mi tutor de proyecto en la universidad y he de agradecerle su dedicación y apoyo a lo largo de mis estudios en la Politécnica.

# Índice general

# Índice de figuras

# Capítulo 1

# OBJETIVOS Y MOTIVACIÓN

## 1.1. Introducción

Las redes inálambricas han revolucionado los intercambios de datos y definido un nuevo paradigma, el del *"Always On-Always Connected"*. Dentro de este paradigma, las comunicaciones en entornos vehículares abren un nuevo campo de investigación en la comunidad científica.

La forma más común de considerar las redes inalámbricas es aquella en la cual los clientes móviles se conectan a una estación base (BS) que controla las comunicaciones. Esta BS cubre una cierta área de cobertura en la cual todos los clientes que controla pueden comunicarse entre sí. El alcance a clientes de otras redes se hace a través de un segmento generalmento fijo. Los clientes son capaces de desplazarse y de cambiar de BS sin corte de cobertura mediante un proceso llamado handover.

Las comunicaciones ad-hoc, y más precisamente las comunicaciones VANETs (*"Vehicular Ad-Hoc Network")* plantean nuevos retos. En este tipo de redes no existe infraestructura de red sino que se compone de los propios nodos móviles autónomos comunicándose entre sí por enlaces inalámbricos. En este entorno desaparece el control centralizado de la red que proporcionaba la BS. Los nodos deben asumir responsabilidades de encaminamiento y de mantenimiento de la red.El control de red está distribuido entre los mismos nodos.

A esos nuevos retos de control de red se suman las características de topologías del entorno vehícular.Las características de las redes vehículares son en general hostil al intercambio de tráfico. El proceso de encaminamiento no se puede asumir de la misma manera que en las redes clásicas. Es necesario que cada nodo por separado y todos en su conjuntos sean capaces de proporcionar un mecanimo dinámico de encaminamiento. Este encaminamiento multihop

se basa en las capacidades de cada nodo. Los protocolos de encaminamiento clásicos no sirven en ese entorno ya que no están preparados para variaciones de topología, puede que no converjan.En tal entorno, el envío de paquetes entre nodos se vuelve todo un reto.

## 1.2. Objetivos

El WG IETF MANET [W1] ha permitido la creación de varios protocolos de encaminamiento para el entorno vehícular como estándares. A pesar de esos esfuerzos aún existe mucho trabajo por realizar.El objetivo de este trabajo es proporcionar una comparativa del rendimiento de los diferentes protocolos de encaminamiento para las comunicaciones entre vehículos, también conocidas como *"vehicule-to-vehicule Communications"* (V2V) o *"Vehicular Ad Hoc Networks"* (VANET).

Para llevar a cabo este estudio comparativo nos centraremos en primer lugar en definir una plataforma de simulación que nos permita simular escenarios reales de comunicaciones VANET. Una vez implementada la plataforma de simulación será necesario especificar escenarios de comunicaciones para las simulaciones Esos escenarios nos permitirán obtener resultados empíricos del rendimiento de los protocolos de encaminamiento en redes VANET que sean unicast o multicast.

La plataforma a definir constará también de un enlace de respaldo sobre tecnología UMTS. Gracias a un proceso de monitarización continua del estado de los enlaces de comunicaciones de la red, cada equipo decidirá en cada momento en que enlace se debe mandar la información, bien por el enlace VANET o bien por el enlace de respaldo UMTS. Si el escenario implica comunicación con el exterior y que no se llega a una pasarela con acceso a Internet por la VANET, se mandará por el enlace de respaldo celular; en el resto de los casos se usarán comunicaciones VANET.

Los escenarios se verán simulados en caso de que se disponga del enlace de respaldo UMTS por un lado y por otro lado los mismos escenarios serán probados en comunicaciones VANET pura. Este hecho nos permitirá comprobar si la introducción de un enlace de respaldo celular mejora de forma significativa los resultados en cuanto al rendimiento de los protocolos.

En cada estudio se harán comparativas de los diferentes protocolos con indicadores como el porcentaje de éxito, el retardo extremo a extremo, el overhead... Esta comparativa de indicadores se mostrará de forma gráfica.

Por último , a la luz de esos indicadores y gráficas podremos concluir y discutir sobre el mejor rendimiento de un protocolo que otro en escenarios específicos.

## 1.3. Requisitos de la solución propuesta

En este apartado se describen los requisitos mínimos a los cuales se deberá ajustar la solución propuesta para resolver el problema previamente planteado. Dada la multitud de propuesta en cuanto a programas de simulación de red y la variedad de escenarios posibles se tendrá que definir de manera concreta los requisitos de la solución contemplada. De un lado, se comentarán los requisitos que la plataforma de simulación debe cumplir para proporcionar un entorno fiable para las simulaciones. Por otro lado, se definirán requisitos de topología de redes para cada escenario.

### 1.3.1. Requisitos de la plataforma de simulación

Para cumplir de manera satisfactoria los requisitos de este proyecto la plataforma de simulación debe presentar características específicas. Estos requisitos son:

- Los diferentes programas que componen la plataforma deben ser libres y de código abierto. Este requisito es fundamental por dos razones. Primero, por razones econónomicas obvias;el carácter libre del código nos libera de la necesidad de pagar licencias. Por otro lado, es necesario que sea de código abierto para temas de flexibilidad a la hora de modificar partes del código si fuese necesario para alcanzar nuestros objetivos de simulaciones.

- Es necesario tener implementado en el simulador todos los protocolos elegidos para la comparativa.

- Es necesario disponer de herramientas que nos permitan especificar de forma rápida los escenarios que nos proponemos simular. Esas herramientas nos deben proporcionar la posibilidad de definir patrones de movimiento de los vehículos, de variar el número de nodos...etc.

- Es necesario que el simulador proporcione indicadores de rendimiento de red o en el caso de que no sea posible debe proporcionar trazas para permitir la extracción de los valores de tales indicadores.

- A partir de los indicadores o de las trazas obtenidas será necesario disponer de una herramienta que permita representar de forma gráfica los valores de los indicadores.

- Es útil que el simulador disponga de un animador gráfico. Esta herramienta muestra de forma gráfica y dinámica como se ha producido la simulación, los movimientos de los nodos, los paquetes perdidos...etc. Ese requisito no es esencial sino deseable ya que no proporciona una forma más visual de ver los flujos de red.

### 1.3.2. Requisitos de topología

El objetivo final de ese proyecto es obtener una comparativa de los protocolos de encaminamineto en entornos vehiculares, por lo cual los escenarios a definir deben ser aproximaciones de la situaciones reales de este entorno. Por lo tanto se han elegido dos topologías típicas: un circuito urbano y una autopista, cada una con tres densidades de tráfico diferentes.

#### Circuito urbano

Este circuito debe tener unas características las más cercanas a un tramo de vía real.

- Un único sentido de circulación con dos carriles.
- Velocidades absolutas de los vehículos entre 50 y 80 km/h.
- Curvas cerradas (90 grados).

#### Autopista

Al igual que en el caso del circuito urbano se debe considerar situaciones las más realistas posibles. Sin embargo, considerar una autopista en su integralidad nos llevaría a un consumo de tiempo y de memoria considerable. Por lo tanto, consideraremos un tramo bastante significativo de las comunicaciones intercambiadas en ese entorno y aproximaremos el comportamiento total considerando que corresponde a la suma de los comportamientos individuales simulados. Los requisitos son los siguientes:

- 3 Kms de recorrido.
- Dos sentidos de circulación próximos entre sí, con dos carriles por sentidos. Cada sentido separado por una mediana de 10 metros de longitud.
- Velocidades absolutas de los vehículos entre 100 y 120 Km/h.
- Tramos muy uniformes, sin fuertes pendientes y con radios de curvatura muy elevados.

## 1.4. Descripción de los capítulos

En el capítulo 2 nos ocuparemos de describir los avances en el campo de las redes VANETs hasta la fecha de hoy. Describiremos las características principales de las VANETs, las tecnologías implicadas en su desarrollo y los aspectos a investigar. Nos detendremos con particular atención en describir

los protocolos de encaminamiento que se han desarrollado para este tipo de redes, dado que este tema es el eje central de nuestro proyecto. Por fin, describiremos los principales servicios que se esperan desarrollar sobre las redes vehículares.

En el tercer capítulo definiremos los escenarios de comunicación a simular. Es decir estudiaremos que pruebas queremos llevar a cabo. En segundo lugar, definiremos indicadores para poder comparar los resultados de las pruebas consideradas.

El capítulo 4 se centra en la plataforma de simulación que hemos desarrollado para llevar a cabo este proyecto. Se describen los programas utilizados, sus instalaciones y el funcionamiento de la plataforma de simulación. Luego, se detallan las modificaciones efectuadas al código fuente original para la perfecta adecuación a nuestros objetivos.

En el capítulo 5, presentaremos los resultados a las simulaciones realizadas. A partir de los escenarios definidos en el capítulo 3, nos centraremos primero en una comparativa de los protocolos unicast, seguido de un estudio de los protocolos geocast para acabar finalmente con un estudio de un red VANEt con respaldo UMTS. Intentaremos demostrar que la introducción de un enlace de respaldo UMTS es una mejora significativa para la red VANET.

Finalmente, en un último capítulo nos detendremos para resumir los logros obtenidos en este proyecto. Examinaremos los objetivos cumplidos y los beneficios aportados al campo de las VANETs. Miraremos también al futuro heciendo mención de las líneas de trabajo a explorar en un futuro a medio o largo plazo.

# Capítulo 2

# ESTADO DEL ARTE

En este capítulo vamos a intentar dar una visión general de los desafíos que plantean las VANETs e expondremos algunas de sus aplicaciones. Siendo muy conscientes de la envergura de la investigación actual sobre estos temas, y de las limitaciones de cantidad de información que podemos aportar, nos limitaremos a una exposition muy superficial, y quedarían muchos temas por abordar en particular en cuanto a seguridad y calidad de servicio. El único aspecto que trataremos de manera más detallada es el encaminamiento en redes VANETs por ser directamente vinculado con nuestro proyecto.

## 2.1. Redes VANETs

Las redes VANETs son un caso particular de las redes ad-hoc (*Mobile Ad-hoc Network (MANET)*) enfocadas a entornos vehiculares. Se trata de un conjunto de nodos que se comunican entre sí mediante enlaces inálambricos sin la necesidad de una infraestructura de red fija. Cada nodo actúa como router y tiene capacidades de encaminamiento para redirigir paquetes hacía su destino.

### 2.1.1. Características

Veamos a continuación el conjunto de características de estas redes:

- Autonomía. Cada nodo es un nodo autónomo con capacidad de procesado de la información que se intercambia en la red. El control de la red no depende de una infraestructura externa sino que se distribuye en todos los nodos de la red siendo así más tolerante a fallos.

- Encaminamiento distribuido. De la misma manera que son autonómos, los nodos deben ser capaces de encaminar información, deben tener ca-

pacidades de router. Por lo tanto, es necesario definir nuevos protocolos de encaminamiento capaces de soportar esa característica.

- Topología de red variable. En una MANET los nodos se pueden mover de forma arbitraria. Esa característica se debe matizar en el caso de las VANETs ya que los vehículos suelen seguir un cierto patrón de movimiento, por ejemplo siguiendo las curvas de un circuito urbano. Aún así, los vehículos se mueven de forma más rápida que un terminal en una red móvil clásica. Debido a esa variabilidad de posición se pueden producir pérdidas importantes de paquetes. Serán necearios mecanismos que detecten estas circunstancias y minimicen sus efectos.

- Capacidad variable de los enlaces. Esta característica tiene cabida en todas las comunicaciones inalámbricas, pues es intrínseca al medio de transmisión pero sus efectos se agravan más en las MANETs. Esto se debe a que cada nodo actúa como router y la información atreviesa múltiples enlaces inámbricos.

- Terminales limitados. En la mayoría de los casos los nodos de este tipo de redes serán terminales ligeros embarcados en vehículos con capacidades limitadas de procesamiento, comunicación y alimentación por lo que es primordial que los algoritmos utilizados optimicen estos tres recursos.

### 2.1.2. Desafíos

Las características de las redes VANETs y más generalmente de las MANETs abren un nuevo campo de investigación para la comunidad científica ya que no se han resueltos muchos de los problemas que plantean ese tipo de redes. Veamos a continuación una serie de temas que quedan abiertos a la investigación:

- Encaminamiento. Existe una movilidad constante en las redes VANETs, lo que supone cambios extremadamente rápidos de la topología de la red e implica una necesidad de reconfigurar las tablas de encaminamiento presentes en cada nodo. En este estudio expondremos con detalles las propuestas de soluciones que se han dado para paliar ese problema.

- Seguridad. Para poder acceder a una red cableada, un usuario tiene que tener acceso físico al cable. Sin embargo, las comunicaciones inálambricas, ya que usan el aire como canal de comunicación, son débiles en cuanto a consideraciones de seguridad. Ese problema se ve agravado en las VANETs ya que no existe infraestructura que pueda centralizar los servicios de seguridad, como puede ser la autenticación de usuarios

o el cifrado de los paquetes por ejemplo. Se sigue investigando para proporcionar mecanismos de seguridad a ese tipo de redes.

- Calidad de servicio (QoS). La calidad de servicio en redes cableadas se proporciona mediante mecanismos de reserva de recursos. Sin embargo, la reserva de recursos se complica con la variabilidad de la topología de las VANETs. Además ninguna red puede prescendir de QoS ya que las aplicaciones de tiempo real como la videoconferencia o el videostreaming exigen un nivel alto de QoS. Actualmente existen propuestas, sin embargo muchas de ellas son teóricas, simuladas o implementadas con pocos nodos, y ninguna de ella aporta una solución definitiva.

- Consumo de potencia. Hemos destacado previamente el carácter ligero de muchos terminales de la red, por lo cual es importante optimizar los procesos de comunicación y procesamiento para garantizar un bajo consumo de energía. Este recurso depende mucho de la tecnología usada.

### 2.1.3. Tecnologías inalámbricas usadas en redes VANETs

En este aparto se detallan tecnologías inalámbricas susceptibles de dar soporte a redes VANETs.

#### Tencología IEEE 802.11

Más conocida como WiFi, se basa en el estándar IEEE 802.11. Opera en bandas libres. Las versiones b y g se han extendido mucho hasta el punto de que la mayoría de los equipos portátiles y PDAs la traen incorporada de serie. Tiene un alcance de unas centenares de metros y un ancho de banda de hasta 54 Mbps, dependiendo de la versión del estándar. La nueva versión, 802.11n pretende aumentar las tasas de transferencia hasta un 500Mps. La seguridad forma parte de los protocolos desde el principio y fue mejorada en la revisión 802.11i

#### 802.11p

También conocida como *Wireless Access for the Vehicular Environment (WAVE)*, está en proceso de estandarización y será la encargada en un futuro de soportar las comunicaciones vehiculares. WAVE es una evolución del estándar IEEE 802.11a con modificaciones a nivel físico y MAC para mejorar su comportamiento en el entorno vehicular y dar soporte a sistemas de transporte inteligente (*Itelligent Transportation Systems (ITS)*).Asimismo, WAVE será la base sobre la que se desarrollará el DSRC (*Dedicated Short*

*Range Communications*), otro proyecto de estandarización impulsado por el ministerio de transporte de EE UU y por un número importante de fabricantes de la industria automóvil, cuyo objetivo es crear una red nacional de comunicaciones vehiculares. El propósito del proyecto es definir un estándar para las comunicaciones V2V y las comunicaciones con la infraestructura vial (V2I) que se puede instalar en semáforos o paneles de información, por ejemplo. La fecha de publicación de la primera versión del estándar está prevista para Abril 2009.

WAVE pretende aumentar las tasas de trasferencia a corto alcance, tipicamente entre 100 y 500m. La técnica de modulación se basa en IEEE802.11a, utilizando OFDM pero con tasas de transmisión de 3, 4.5, 6, 9, 12, 18, 24 y 27 Mbps en canales de 10MHz. Utiliza 52 sub-portadas moduladas utilizando BPSK, QPSK, 16-QAM, o 64-QAM.

En cuanto a la canalización, la norma define 7 canales no solapados de 10MHz en la banda de 5.9 GHz: 6 canales de servicio (SCH) y uno de control (CCH). El CCH está utilizado como canal de referencia para realizar una primera detección de los vehículos cercanos como paso previo al establecimiento de las comunicaciones. Al mismo tiempo, dicho canal se usa para anunciar los servicios disponibles en canales SCH (acceso a Internet, descarga de contenidos..etc.) El canal CCH se usa para la transmisión en modo broadcast de mensajes de seguridad vial. Este contenido es prioritario sobre los demás tráficos y se transmite en el canal CCH con una tasa de datos de 6Mbps, correspondiente a una modulación QPSK con un ratio de codificación de $1 \setminus 2$.

En la capa MAC, WAVE se basa en las definiciones del IEEE802.11 usando una técnica de acceso basada en CSMA/CA (*Carrier Sense Multiple with Collision Avoidance*). Sin embargo, CSMA/CA no logra solucionar el problema del términal escondido.


Figura 2.1: Problema del terminal escondido

Como podemos observar en la figura 2.1, la estación 1 y la estación 3 intentan mandar tráfico al mismo instante a la estación 2, ya que no se escuchan, no tienen alcance la una a la otra. Se produce entonces colisiones de paquetes. El problema del terminal escondido surge siempre cuando dos nodos se hallan fuera del alcance radio entre ellos e intentan mandar información a un mismo nodo en un mismo instante. Para tratar ese problema se implementa un mecanismo de intercambio de mensajes RTS/CTS (*Request-to-Send/Clear-to-send*). Antes de mandar datos, la estación 1 manda una

trama RTS al destino para indicar que desea mandar tráfico. La estación 2 recibe el RTS e informa al resto de los nodos a su alcance que va a reservar el canal para la comunicación con la estación 1. De esta forma la estación 3 queda informada que tiene que esperar antes de mandar paquetes. Podrían darse casos de colisiones de paquetes RTS, sin embargo el efecto sería reducido ya que se tratan de paquetes de pequeño tamaño (hasta 2347 octetos).

Este mecanismo evita colisiones pero introduce una sobrecarga de tráfico en la red y retardo en las transmisiones. Por esas razones, WAVE no implementa RTS/CTS en el canal CCH por transmitir en modo broadcast. Como consecuencia, todos los nodos que utilizan el canal de control están sujetos al problema del terminal escondido, incrementando el riesgo de pérdidas de paquetes y de congestión de canal.

### Bluetooth

También conocido como 802.15.1. Es la tecnología más extendida en cuanto a comunicaciones inalámbricas personales ($wPAN$). Hay varias clases dependiendo de su alcance y consumo de potencia, alcanzando tasas de 2Mbps y rangos de hasta 100m. Opera en banda libre y sus mecanimos de seguridad son suficientemente robustos.

### UWB

Ultra Wide Band es un estándar basado en 802.15.3 que funciona emitiendo a muy baja potencia en un espectro enorme. Su alcance es muy limitado (<10m) pero proporciona tasas de transferencia muy elevadas llegando a los 480 Mbps. Su consumo de energía es muy reducido.

### ZigBee

Es la tecnología más utilizada en redes de sensores ad hoc. Se basa en el estándar 802.15.4. Presenta anchos de banda muy pequeños y cobertura reducidas (250 Kbps hasta 75m). Es de gran utilidad para enviar poca información en pequeñas distancias. la gran ventaja es que su consumo es extremadamente reducido.

A continuación se muestra una tabla con las características más relevantes de cada tecnología:

Cuadro 2.1: Características de las tecnologías inalámbricas consideradas

| ***Tecnología*** | ***Cobertura*** | ***Tasas*** | ***Consumo*** |
|---|---|---|---|
| 802.11b | 500m | 11 Mbps | Alto |
| 802.11g | 500m | 54 Mbps | Alto |
| WiMAX (802.16e) | 50 Kms | 75 Mbps | Alto |
| Bluetooth (802.15.1) | 20m | 2 Mbps | Medio |
| UWB (802.15.3) | <10m | 480 Mbps | Bajo |
| Zigbee (802.15.4) | 75m | 250 Kbps | Muy bajo |

### 2.1.4. NFC

*"Near Field Communication"*, NFC es una nueva tecnología de comunicación inalámbrica que proviene de la combinación de varias tecnologías de identificación e interconexión.

NFC provee una forma de comunicación entre dispositivos electrónicos, como pueden ser los teléfonos móviles, las PDAs...etc. La comunicación se realiza entre dos dispositivos de forma *"peer-to-peer"*.Trabaja en la banda de los 13.56 MHz, banda que no necesita compra de licencia para su uso. El alcance de NFC es extremadamente corto, se usa para comunicaciones de dispositivos que se encuentran a menos de 4 cm de distancia. Dado ese rango muy corto de cobertura, las comunicaciones son de forma inherente totalmente seguras. Las tasas de transferencia son de hasta 424 Kbps.

Según el entorno de los dispositivos se negocia las velocidades de transferencia y se puede reajustar ese parámetro en cualquier momento de la comunicación.

En entorno vehicular, NFC ofrece muchas posibilidades de aplicación. Podemos citar por ejemplo, el pago de peajes, el uso del dispositivos como llave integrada, control de acceso a servicios de ocio...etc. NFC goza de una gran aceptación por parte de fabricantes e industrias del sector en general, por lo cual se espera una gran implementación en todo tipo de dispositivos de comunicación en un futuro.

## 2.2. Protocolos de encaminamiento

### 2.2.1. Introducción

La investigación en el campo de los protocolos de encaminamiento para redes ad-hoc se ha multiplicado estos últimos años. La movilidad de los

nodos, la inestabilidad de las topologías, y la ausencia de una infraestructura de centralización hacen obsoletos los protocolos que se usan en redes fijas. En redes ad-hoc, los protocolos de encaminamiento deben ser capaces de funcionar de manera automática y distribuida.

A la hora de clasificar los protocolos de encaminamiento existen varios criterios. Se puede considerar :

- El alcance: unicast, broadcast o multicast, geocast, etc.
- El modo de descubrimiento de rutas : proactivo, reactivo, híb rido.
- Tipo de algoritmo que implementan : vector de distancias, estado de enlace.

### 2.2.2. Clasificación

#### Basada en el alcance

Se distinguen dos familias de protocolos: los protocolos unicast y los protocolos multicast.

Los protocolos unicast son los que transmiten información de un único destino a un único receptor. En contraposición, los multicast envían la información a un grupo de nodos.

El multicast consiste en mandar simultáneamente información a múltiples destinos, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de red. Antes del envío de la información, deben establecerse una serie de parámetros. Para poder recibirla, es necesario unirse a lo que se denomina "grupo multicast". Ese grupo multicast tiene asociado una dirección. En IPv4, por ejemplo, se reservan las direcciones de tipo D para la multidifusión (224.0.0.0 a 239.255.255.255). Dentro de los protocolos multicast hay casos particulares que son interesantes de destacar: el caso del protocolo broadcast,el protocolo geocast, y el anycast.

El protocolo broadcast manda información a todos los nodos dentro de su alcance radio, por lo cual no es necesario haberse unido al grupo multicast previamente. El anycast manda información a un destinatario único, pero uno cualquiera no especificado. Un caso de multicast de grande importancia en las redes MANETs es el geocast, consiste en mandar tráfico a un grupo de receptores situado en una misma zona geográfica. En este caso no es necesario unirse a un grupo previamente, solo por su posición geográfica de un nodo recibirá o no los paquetes enviados.

### Basada en el modo de descubrimiento de rutas

Para descubrir las rutas hacia los destinos de la red, las MANETs usan dos esquemas distintos: el esquema reactivo y el esquema proactivo.

Los protocolos proactivos intentan tener en cada momento, y independientemente de las necesidades de encaminamiento, una visión precisa del estado de la red. Se busca mantener actualizadas las tablas de encaminamiento a través del envío de mensajes de forma periódica. Esta característica procura una respuesta rápida ante solicitudes de ruta y suele ofrecer un buen comportamiento en los escenarios de movilidad alta. Sin embargo, para mantener una actualización permanente de las rutas, se introduce una sobrecarga importante de la red con los mensajes de control.

Por otro lado, existen los protocolos reactivos, que que sólo obtienen información de encaminamiento cuando es necesario. Son protocolos bajo demanda que buscan la ruta hacia un destino en el momento en el que se quiere mandar información a ese destino. Obviamente, en las redes que usan esos tipos de protocolos la sobrecarga es menor que para los protocolos proactivos. Sin embargo, los retardos al establecimiento de las comunicaciones son mayores.

Existen protocolos híbridos que combinan esos dos esquemas utilizando, por ejemplo, proactividad en las cercanías del nodo considerado pero buscando las rutas bajo demanda para los nodos más alejados.

En todos casos, la eficiencia del mecanismo depende del escenario y del patrón de movimiento considerado. Hay que llegar a un compromiso entre la frescura de las rutas, el overhead y la latencia en descubrimiento. En este proyecto, intentaremos definir la eficiencia de los protocolos en distintos escenarios.

### Basada en el algoritmo implementado

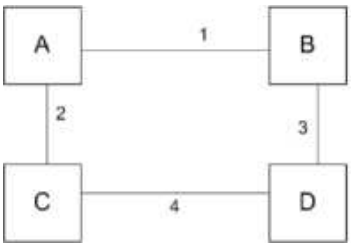
Atendiendo al tipo de información intercambiada podemos hablar de dos familias de protocolos : estado de enlace y vector de distancia.

En un protocolo basado en el vector de distancia, cada nodo mantiene una tabla de encaminamiento de este estilo:

| ***Desde A hasta*** | ***Enlace*** | ***Coste*** |
|---|---|---|
| A | Local | 0 |
| B | 1 | 1 |
| C | 2 | 3 |
| D | 2 | 5 |

Periódicamente, cada nodo pasa su tabla a sus vecinos. Con la información recibida, cada nodo recalcula su tabla.

Por otro lado, encontramos los protocolos basado en el estado del enlace. Todos los nodos mantienen una tabla del mapa completo de la red.




| ***Desde*** | ***Hasta*** | ***Enlace*** | ***Distancia*** |
|---|---|---|---|
| A | B | 1 | 1 |
| A | C | 2 | 1 |
| B | A | 1 | 1 |
| B | D | 3 | 1 |
| C | A | 2 | 1 |
| C | D | 4 | 1 |
| D | B | 3 | 1 |
| D | C | 4 | 1 |

Cada nodo manda periódicamente el estado del enlace con sus nodos vecinos . El nodo A mandaría *<B,1,1><C,2,1>*.Los mensajes se inundan en la red por todos los enlaces salientes. A la recepción de una tabla de número de secuencia X:

- Si X es superior al número actual de mapa, se actualiza la tabla y se reenvía.
- Si X es inferior al número actual de mapa, se manda el mapa actual por el enlace de llegada del mensaje.
- Si X es igual al número actual de mapa, no se hace nada.

Con las tablas conseguidas, cada nodo aplica el algoritmo de Dijkstra para calcular las rutas óptimas.

En ese proyecto, hemos elegido basarnos en una clasificación basada en el alcance de los protocolos. Nos parece la mejor manera de dividir las pruebas ya que queremos saber cual es el mejor protocolo para un escenario concreto,

independientement de su algoritmo o de su esquema de descubrimiento de rutas. En cada escenario se quiere probar un determinado tipo de comunicaciones : unicast, geocast... etc.

Los protocolos que vamos a estudiar con más profundidad son:

- Broadcast: Flooding,MPR, NES, CDS
- Unicast: DSDV, DSR, AODV, LAR, TORA, ZRP, OLSR y FSR
- Multicast: MAODV
- Geocast : LBM, GeoTORA, GeoGRID, y Gamer.

Se han elegido esos protocolos por ser representativos de su grupo, por ser los más usados o por haber trabajado con ellos a nivel de simulación.

Cuadro 2.2: Características de los protocolos

| ***Protocolo*** | ***Alcance*** | ***Esquema*** | ***Información geográfica*** |
|---|---|---|---|
| Blind Floodig | Broadcast | - | No |
| MPR | Broadcast | - | No |
| NES | Broadcast | - | No |
| CDS | Broadcast | - | No |
| DSDV | Unicast | Proactivo | No |
| DSR | Unicast | Reactivo | No |
| AODV | Unicast | Reactivo | No |
| LAR | Unicast | Proactivo | Sí |
| TORA | Unicast | Reactivo | No |
| ZRP | Unicast | Híbrido | No |
| FSR | Unicast | Proactivo | No |
| OLSR | Unicast | Proactivo | No |
| MAODV | Multicast | Reactivo | No |
| LBM | Geocast | Proactivo | Sí |
| GeoTORA | Geocast | Reactivo | Sí |
| GeoGRID | Geocast | Reactivo | Sí |
| GAMER | Geocast | Proactivo | Sí |

### 2.2.3. Protocolos Broadcast

[FIDSIS 2005]

El broadcasting consiste en mandar tráfico desde un nodo origen a todos los nodos presentes en la red usando la técnica de múltiples saltos.

### Blind-Flooding

El protocolo lo más simple es el *"Blind-Flooding"*. A la recepción de un mensaje, un nodo lo reenvía a todos sus vecinos. La única optimización que presenta este protocolo es que cada nodo recuerda los paquetes flooding que ha recibido y si le vuelven a llegar no los retransmite evitando así duplicidades. Aunque sea muy simple de implementar, el *"Blind Flooding"* introduce mensajes redundantes y colisiones a nivel MAC que empeoran el rendimiento de la red.

### Multi-Point Relay Flooding (MPR)

MDR consiste en elegir un conjunto de nodos vecinos que cubre el acceso a los nodos distantes de 2 saltos. Los nodos de ese conjunto reenvían el tráfico, los demás no. Esa mejora permite dividir por 2 el número de mensajes de control.

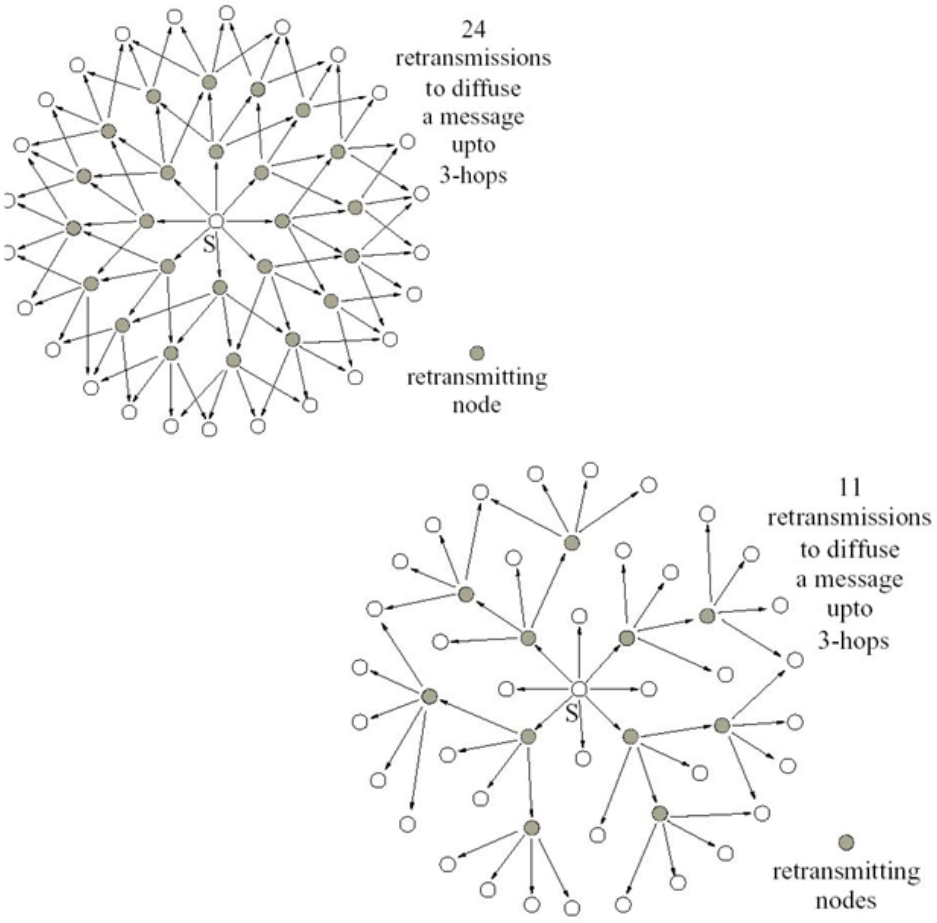



Figura 2.2: Mejoras de MPR frente a Blind-Flooding

### Neighbor Elimination Scheme (NES)

Un nodo que recibe un mensaje de broadcast no retransmite directamente sino que espera un tiempo aleatorio para ver si otro nodo manda la información. Los nodos escuchan los mensajes y apuntan que nodos ha mandado información a cual otro. Después del tiempo de espera, el nodo manda el tráfico a sus vecinos que no han sido informados por otros nodos. En la figura 2.3 se puede ver como B después de un tiempo de espera se da cuenta de que no es necesario mandar tráfico a ningún nodo.

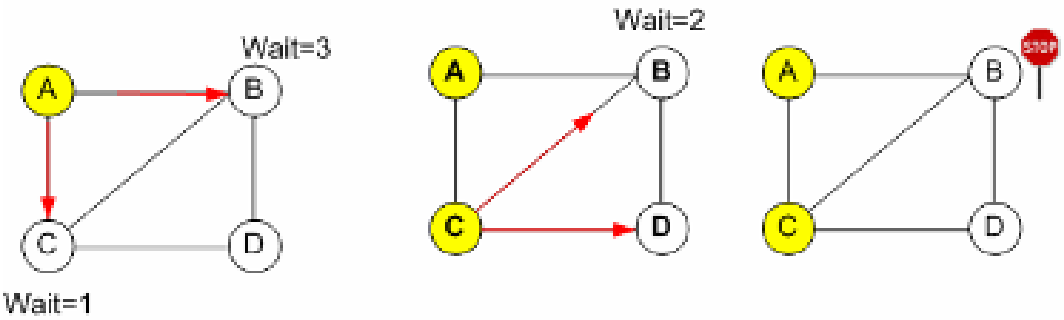



Figura 2.3: Mecanismo NES

### Connected Dominating Sets (CDS)

[JBMDATXC 2004]
La idea de este mecanismo es organizar los nodos de la VANETs en una jerarquía. Se hace una clasificación de los nodos en dos categorias : los nodos dominantes y los nodos pasivos. Los nodos dominantes son elegidos de manera que cubran la totalidad de la red en sus retransmisiones. Existen varias formas de construir la jerarquía dentro de la red. La más simple y conocida es la siguiente:

Se asigna una prioridad a cada nodo. Un nodo es pasivo si dentro de sus vecinos directos existe un nodo de prioridad superior que ya cubre el vecindario. Si no es el caso, el nodo es dominante. La asignación de prioridades a los nodos es un mecanismo complicado que usa algoritmos matemáticos complejos que no vamos a detaller aquí. A la recepción de un mensaje broadcast un nodo retransmite ese mensaje solo si se trata de un nodo dominante.

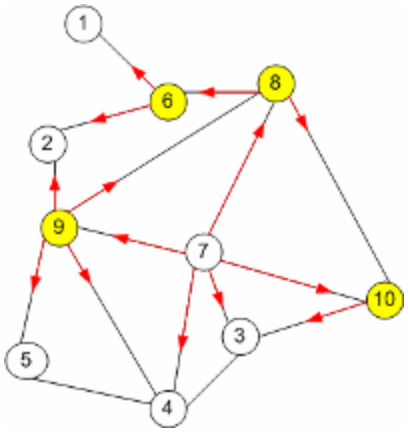



Figura 2.4: Mecanismo de CDS

### 2.2.4. Protocolos unicast

#### DSDV

*Destination-sequenced Distance-Vector Routing (DSDV)* [CEPPB 1994] es un protocolo unicast proactivo adaptado del tradicional RIP (*Routing Information Protocol*). Su principal objetivo es evitar los problemas de bucles en la actualización de las tablas de encaminamiento. Por lo cual añade un nuevo campo a las tablas RIP, el número de secuencia que permite distinguir entre una tabla antigua y una más reciente.

Como su nombre lo indica, DSDV implementa un algoritmo basado en el vector de distancias. Eso significa que mantiene tablas con todos sus destinos accesibles junto con el siguiente salto, la métrica, y un número de secuencia de la entrada en la tabla generado por el nodo destino.Las tablas se mandan en modo broadcast de forma periódica o cuando ocurre un cambio significativo de la topología de red. Una ruta es considerada mejor que otra si tiene un número de secuencia mayor o, en caso de empate, si la distancia al destino es menor.

Cuando un nodo B detecta que la ruta hacia cierto destino D se ha roto, inunda la red con una actualización de esa entrada en la que se ha incremen-

tado el número de secuencia en uno y la distancia se marca como infinita. Cuando A recibe este mensaje incorpora a su tabla la actualización de la entrada hacia D a través de B siempre que no tuviera una entrada mejor para alcanzar D.

Para conseguir una cierta consistencia en las tablas de encaminamiento de cada nodo al cambiar la topología de la red, las actualizaciones deben ser frecuentes y suficientemente rápidas para que cada nodo pueda tener una visión realista de la red en un momento dado. El problema fundamental de DSDV es la elevada sobrecarga de control que genera. Al no haber una especificación estándar, no hay productos comerciales basados en este protocolo. Sin embargo, es la base sobre cual se han desarrollado otros protocolos como por ejemplo AODV.

### DSR

*Dynamic Source Routing* es un protocolo reactivo unicast. El protocolo se compone de dos mecanismos : el descubrimiento y el mantenimiento de rutas que permiten a un nodo origen descubrir y mantener las rutas hacia un nodo destino cuando se necesita mandar tráfico en la red ad-hoc. Se basa en una técnica de *"Source Routing"*. La idea de esta técnica es determinar la mejor ruta completa hacia un destino. El nodo origen inunda la red con una trama de exploración. Al recibir una replica de la trama exploradora, cada nodo se agrega explícitamente en la cabecera de la trama, y actualiza sus tablas con la información contenida en la cabecera de dicha trama.

El descubrimiento de rutas es el mecanismo por el cual un nodo origen S que desea mandar tráfico a un nodo destino D, obtiene la ruta hacia D. Si S no dispone de ninguna ruta hacia D, empieza un proceso de descubrimiento de rutas mediante un broadcast del *Route Request Packet*(RREQ). Este paquete contiene la dirección de destino, la dirección del nodo fuente y un número único de identificación. Cada nodo que recibe un paquete RREQ, revisa si conoce la ruta hacia el destino. Si no la conoce, se reenvía el paquete. Si la tiene contesta en sentido inverso con un *Route Reply Packet*(RREP). Todos los nodos que participan al reenvío del RREP añaden su dirección en la cabecera del paquete, creando de ese modo la ruta completa hasta el destino.

En cambio, el manteniemiento de rutas consiste en la capacidad de detectar que una ruta almacenada en una tabla ya no se puede usar debido a un cambio de topología. El mantenimeinto de rutas detecta que un enlace en la ruta hacia D ha desaparecido. Se producen paquetes de error *Route Error Packets* en un nodo, cuando la capa de enlace encuentra un problema grave

de transmisión. Este paquete de error contiene las direcciones de los dos nodos que están unidos por el enlace que falló. En este caso, si S conoce otra ruta hacia D se puede usar, o bien se vuelve a invocar el mecanismo de descubrimiento de rutas para remplazar la ruta caída hacia D. El mantenimiento de rutas sólo tiene cabida cuando S está mandando tráfico a D.

DSR es un protocolo totalmente reactivo, opera bajo demanda, lo que implica que no existe ningún tipo de mensaje periódico, lo que permite reducir de forma significativa el tráfico de control en la red y aprovechar más los recursos de red para paquetes útiles. Además cada vez que se lleva a cabo el descubrimiento de rutas, los nodos implicados pueden extraer y almacenar información sobre la topología de red, lo que ahorra muchos mensajes de control.

Para evitar que se produzca el problema de múltiples respuestas simultáneas y optimizar la ruta final, cuando un nodo recibe un RREQ, se introduce un pequeño retardo variable en la respuesta de cada nodo con una ruta en su caché. Antes de responder con una de las rutas conocidas, cada nodo debe efectuar las siguientes acciones:

- Elegir un retardo $d = H \times (h - 1 + r)$, donde h es la métrica (en saltos) de la ruta que se debe enviar, r es un número flotante aleatorio entre 0 y 1, y H es un pequeño retardo constante : $H \geq 2 \times R$,(R es el retardo máximo de propagación en el enlace).

- Retardar la transmisión de un RREP para este nodo por un período igual a d.

- Durante ese período si el nodo recibe otra respuesta mejor a dicho RREQ proveniente de otro nodo, se cancela la respuesta y se retransmite la nueva.

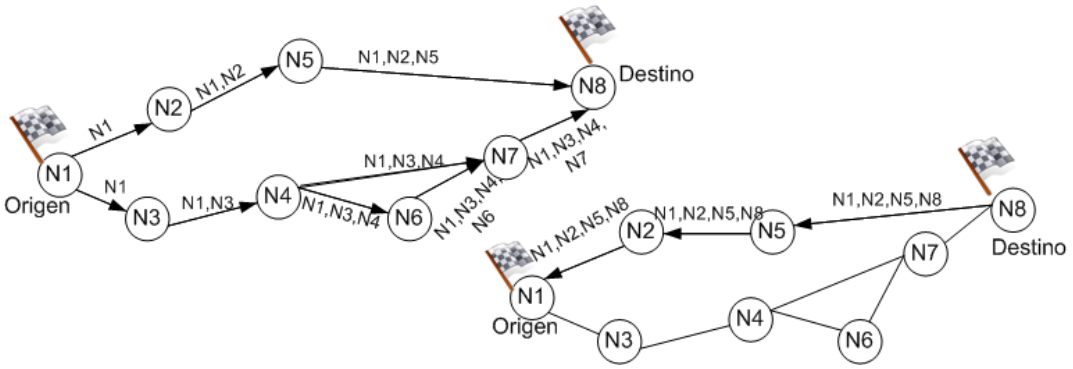



Figura 2.5: Mecanismo de descubrimiento de rutas en DSR

La figura 2.5 ilustra el RREQ por una parte (a la izquierda) y el RREP por otra (a la derecha). En una preocupación de claridad, sólo se ilustra el campo nodo origen de la cabecera del paquete. Es interesante notar como un nodo al recibir dos rutas distintas para un mismo destino elige las menos costosa en cuanto a número de saltos. En estos casos el mecanismo de retardo aleatorio previamente descrito cobra toda su importancia ya que así un nodo es capaz de proveer la ruta óptima al siguiente salto.

### AODV

*Ad-hoc On-Demand Distance-Vector Routing* [CEPERSD 2003] es un protocolo reactivo unicast. Se construye sobre el protocolo DSDV analizado previamente. La idea es mejorar DSDV minimizando el número de paquetes broadcast requeridos para crear rutas, ya que al ser bajo demanda, los nodos que están en el camino no tienen que participar en el intercambio de tablas ni que mantener la ruta. A pesar de ser un protocolo reactivo, AODV tiene la peculiaridad de emitir mensajes alertando sobre su presencia de forma periódica mediante una técnica llamada *Link Layer Feedback*. Esa técnica permite que los nodos tengan conocimiento de sus vecinos más cercanos y mantegan sus tablas actualizadas reflejando los cambios en la topología cercana. Estas tablas se mantienen actualizadas a lo largo del tiempo, eliminando las entradas innecesarias.

Cuando un nodo S quiere transmitir tráfico a un destino D y que no tiene una ruta válida hacia D comienza el mecanismo de descubrimiento (*Path Discovery*). Primero se manda en modo broadcast una petición de ruta,*ROUTE REQUEST (RREQ)* a todos sus vecinos. Este mensaje incluye su propia dirección, la del nodo destino D, y el último número de secuencia recibido de D, en el caso de que se hubiera recibido algún dato con anterioridad.Este mensaje se inunda en la red y los nodos que se atreviesan guardan una ruta inversa hacia S, lo que implica que AODV sólo soporta enlaces bidireccionales. Cuando llega a un nodo que dispone de la ruta hacia D, se comprueba el número de secuencia para el destino D. Si éste es mayor que el incluido en el mensaje, se ha encontrado una ruta válida hacia D. El nodo que dispone de la entrada hacia D manda un mensaje de respuesta (*ROUTE REPLY (RREP))* de vuelta hacia S siguiendo la ruta creada durante la inundación. En este mensaje se incluye el último número de secuencia recibido por el emisor del mensaje RREP. Los nodos que reciben el RREP guardan una entrada hacia D que apunta al nodo que les ha transmitido el mensaje, por lo cual solo se guarda en la tabla el siguiente salto y no la ruta entera. Si pasado un cierto tiempo y que no se ha recibido ningún RREP, S considera que no hay ruta válida hacia D en ese momento.

Las tablas se mantienen actualizadas mientras esté en uso el enlace. Si un nodo origen se mueve, él mismo reinicia el proceso de descubrimiento de rutas. Si un nodo intermediario se mueve, su vecino anterior (en el sentido directo origen-destino) propaga hasta S, un RREP no solicitado con un número de secuencia mayor y con valor de saltos al destino infinitos. De esa manera, S sabe que si quiere seguir usando el enlace tiene que reiniciar el proceso de descubrimiento de rutas.

Cuando no hay tráfico y que se quiere mantener las entradas de los nodos vecinos, se manda mensajes periódicos HELLO, generalmente uno por segundo. Estos mensajes son un tipo especial de RREP no solicitados, cuyo número de secuencia es igual al del último RREP enviado y con un TTL = 1 para no inundar la red sino informar sólo el vecindario. Cuando durante más de tres segundos no se ha recibido ningún HELLO de parte de un vecino se considera el enlace roto y se borra la entrada correspondiente en la tabla de encaminamiento. En la especificacióm de AODV se sugiere la posibilidad de utilizar datos de la capa de enlace o física para determinar el estado de los enlaces, como puede ser por ejemplo escuchar las retransmisiones realizadas por los nodos vecinos.Cada vez que se borra una entrada por rotura del enlace se debe indicar a los nodos que lo usaban como siguiente salto hacia una ruta que deben reanudar el proceso de descubrimiento de rutas. Esto se consigue mediante el *UNSOLICITED ROUTE REPLY* que contiene un valor infinito como distancia hacia el destino y un número de secuencia igual al del último RREP enviado.

### LAR

*"Location Aided Routing"* [YKNHV 1998] es un protocolo proactivo que introduce la idea de enrutamiento geográfico para disminuir la sobrecarga en el descubrimiento de rutas. Esa información geográfica puede ser obtenida usando un sistema de posicionamiento global (GPS, Galileo...), lo que limita el espacio de búsqueda y una diminución de la cantidad de mensajes intercambiados y por lo tanto un incremento del rendimiento de la red.

El algoritmo introduce dos conceptos innovadores: el de *"Expected Zone"* (EZ) y el de *"Request Zone"* (RZ). El protocolo usa el mismo mecanismo de descubrimiento de rutas en cuanto a los mensajes intercambiados que otros algoritmos como AODV o DSDV. La diferencia esencial es que esos mensajes no se mandan a todos los vecinos, sino que a partir de la información geográfica, se consigue una inundación controlada de la red.

Un nodo origen S que quiere descubrir una ruta hacia un destino D, calcula una EZ que corresponde a una previsión de la posición de D. Esa previsión se calcula como una aproximación. S gracias a un sistema como GPS sabe que a un momento $t_0$ el nodo D está en una posición L y que se

mueve a una velocidad media $v$. Por lo tanto, S asume que D al instante $t_1$ se encuentra en la EZ delimitada por el círculo de rayo $v(t_1 - t_0)$ y de centro L. Si además se sabe que D se mueve hacia el norte podemos restringir la EZ al semicírculo como se muestra en la figura 2.6 b).

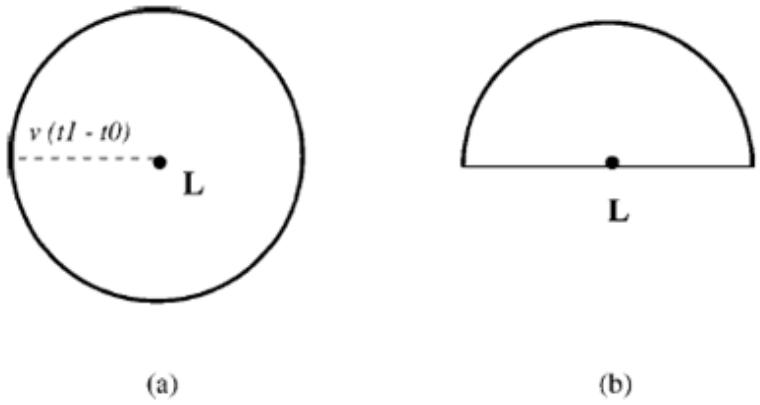



Figura 2.6: Ejemplos de Expected Zone

El segundo concepto es el de *"Request Zone"* (RZ). Corresponde a la zona a la cual se restringe el flooding de descubrimiento de rutas. Para que un mensaje de descubrimiento se mande a un nodo, ese nodo tiene que estar en la RZ. Para aumentar la probabilidad de alcance a D, se han definido reglas de definición de la RZ:

- La RZ debe incluir al nodo origen S, a la EZ y a la región que la rodea.
- Si se elige una RZ muy pequeña puede ocurrir que todas las rutas de S hacia D queden fuera y que el proceso de descubrimiento de rutas se vea afectado de mayor retraso.
- Si se elige una RZ demasiado grande, el mecanismo de rutas puede ser muy costoso e introducir overhead innecesario.

A la luz de esas consideraciones, se ve claramente que existe un compromiso entre la latencia en la determinación de una ruta y la sobrecarga de mensajes diseminados. Uno de los esquemas propuestos es establecer una RZ rectangular, de tal forma que el rectángulo sea el mínimo que contenga a la EZ y al nodo origen ubicado en las coordenadas $(X_s, Y_s)$. El nodo origen puede estar tanto fuera como dentro de la EZ, no influye en el mecanismo. En la figura 2.7, se ven dos nodos J e I, vecinos de S; si el RREQ le llegara a I, éste lo retransmitirá a sus vecinos ya que pertenece a la RZ mientras que si el nodo J, que queda fuera de la RZ, recibe un RREQ, lo rechazará.

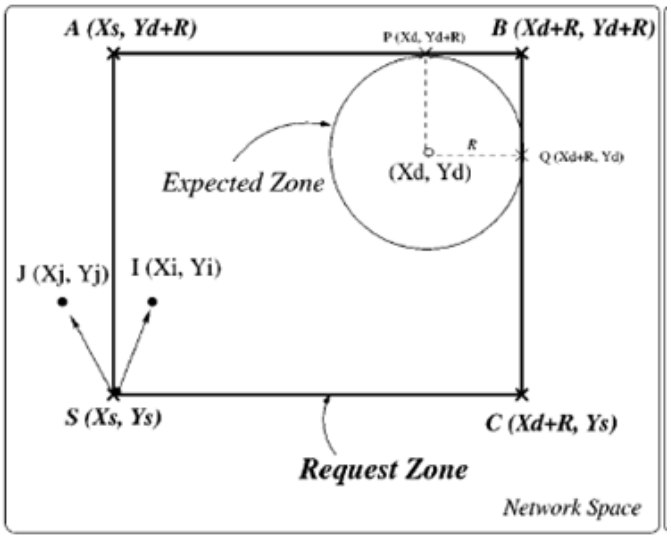



Figura 2.7: LAR con nodo origen fuera de la RZ

### TORA

*"Temporally-Ordered Routing Algorithm"* (TORA) es un protocolo reactivo basado en el concepto de *"Links Reversal"*. Fue propuesto para mejorar las prestaciones en redes altamente dinámicas. La idea básica es la generación de mensajes de control del protocolo en un pequeño conjunto de nodos cerca de la localización de un cambio topológico. El protocolo desarrolla tres funciones básicas: la creación de rutas, el mantenimento y su eliminación.

La fase de creación corresponde a la selección de una métrica para establecer un DAG *("Directed Acyclic Graph")* hacia el destino. El DAG consiste en asignar una dirección a los enlaces basada en las alturas relativas de los nodos vecinos. El nodo origen tiene la altura mayor y el nodo destino la menor. La fase de descubrimiento de rutas es similar a los expuestos anteriormente.

El mantenimiento de rutas se refiere al hecho de adaptar la estructura de encaminamiento en repuestas a los cambios topológicos de la red. Cuando un enlace no está disponible, el DAG se rompe y es necesario una reparación de la ruta para reestablecerlo. El nodo que detecta el fallo en el enlace genera para sus vecinos un mensaje con un nuevo nivel de referencia. Los nodos reaccionan a esa información invertiendo los enlaces hacia el nodo. Haciendo una inversión del sentido de los enlaces, hace que un nodo no contenga el destino y por lo cual la ruta será eliminada. La fase de eliminación de rutas involucra un broadcast de *"clear packet"* (CLR) para eliminar las rutas que no contienen la ruta hacia un destino. TORA elimina las rutas inválidas, busca

una nueva alternativa para un destino, y construye otra ruta en un sólo paso del algoritmo. En cambio, ese mecanismo en AODV o DSR correponde a tres pasos (route error / route request / route reply).

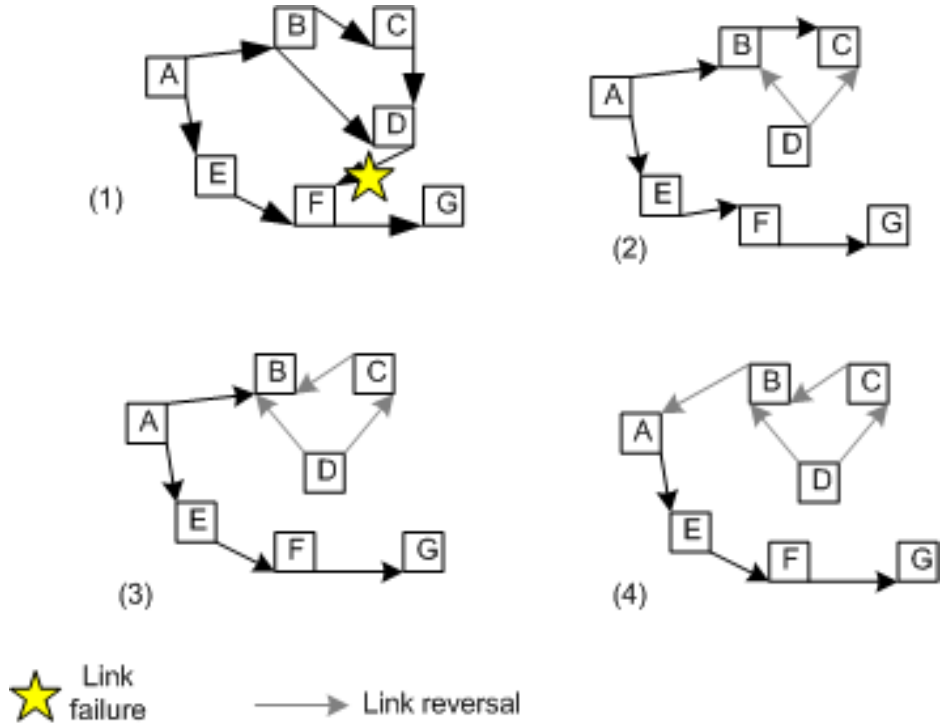



Figura 2.8: Esquema de funcionamiento de TORA

### ZRP

*"Zone Routing Protocol"* [NB 2008] es un protocolo clasificado como híbrido ya que mezcla las capacidades de los algoritmos reactivos y proactivos. Todos los nodos mantienen proactivamente las rutas dentro de una zona local conocida como zona de encaminamiento (IARP). Sin embargo, a nivel global ZRP emplea mecanismos reactivos (IERP) para encaminamar los paquetes entre las áreas locales.

Se define un parámetro llamado Radio de la Zona y que define una zona local de encaminamiento. ZRP mantiene las rutas hacia todos los nodos que se encuentran a una distancia menor o igual al radio de la zona, implementando mensajes "Hello", protocolos de la capa física, etc.

El IERP (*"Interzone Routing Protocol"*) está basado en un mecanismo de distribución de mensajes conocido como *"Bordercast Resolution Protocol"* (BRP). La ventaja de este sistema sobre el broadcasting es que en lugar de

recorrer la red nodo por nodo, BRP permite que las consultas sean dirigidas fuera de la red local y hacia regiones de la red que no hayan sido cubiertas por la consulta. Para llevar a cabo ese mecanismo es necesario tener un control de las consultas para saber que región han sido cubiertas y no volver a mandar mensajes redundantes. .Cuando un nodo detecta que un nodo ha mandado una consulta, todos los miembros de su zona vecindario se marcan como cubiertos.

Para mandar tráfico el nodo comprueba si el destino está en su tabla de encaminamiento local. Si no, manda una consulta mediante el algoritmo de bordercast. Cuando un nodo recibe la consulta, verifica si el nodo está en su zona o si tiene alguna ruta válida hacia el destino. Si la respuesta es afirmativa, el nodo enviará un RREP (Route Reply) hacia la fuente. Si la respuesta es negativa se difunde la consulta a sus vecinos mediante el bordercast.

Para que el protocolo funcione de manera correcta es importante que el radio de la zona sea adecuado al tipo de red en cuestión. Se recomiendan radios pequeños para redes densas compuestas de grupos con pocos nodos que se mueven rápido, y radios mayores para redes dispersas de nodo con movilidad más baja.

### OLSR

*"Optimized Link State Routing"* [TCPJ 2003] es un protocolo proactivo basado en el estado de enlace. OLSR es una optimización directa del algoritmo de estados de enlace adaptado a los requisitos específicos de una WLAN con alta movilidad. La optimización consiste principalmente en la reducción del tamaño de las tablas de enlaces intercambiadas así como del número de retransmisiones necesarias durante los periodos de inundación. La clave del algoritmo reside en el uso de retransmisiones multipunto (MPR). El mecanismo MPR ha sido descrito en el apartado 2.2.3.

Los nodos intercambian periódicamente mensajes HELLO con sus vecinos que permiten detectar la presencia de un nodo vecino así como recoger información relativa al estado del enlace con ese vecino. En los mensajes HELLO se pueden incluir información indicando que el nodo es un nodo MPR. Usando esa información cada nodo elige dentro de su conjunto de vecinos un subconjunto que declara subconjunto MPR. Así , cada nodo tiene conocimiento de un subconjunto de nodos MPR que le permite tener conectividad con todos los nodos distantes de uno o dos saltos. De este modo, sólo los nodos MPR se encargarán de retransmitir los mensajes broadcast.

Para descubrir la topología de la red, los nodos intercambian información acerca del estado de enlace que los conectan con los nodos MPR. Los intercambios son periódicos o generados por eventos relativos a ruptura de enlace. Incluir en las tablas sólo los enlaces a los nodos MPR reduce el tamaño de las mismas, lo que permite reducir el ancho de bando consumido durante su intercambio. Al mismo tiempo permite que las rutas que se vayan creando a posteriori sean óptimas en cuanto a números de saltos ya que sólo usan nodos MPR. OLSR se adapta bien a redes con gran número de nodos y alta movilidad.

### FSR

*"Fisheye State Protocol"* [MGXH 2002] es un protocolo proactivo basado en el concepto de estado de enlaces. El "Ojo de un pez" es un mecanismo mediante el cual se captura con detalle los píxeles que se encuentran cerca del punto de focal. El detalle disminuye a medida que se aumenta la distancia al punto focal. FSR se basa en una analogía de ese algoritmo. Mantiene distancias exactas y alta calidad de la información relativa a los nodos los más cercanos e pierde progresivamente detalles a medida que la distancia al nodo aumenta.

FSR, de manera similar al algoritmo de estado de enlace manda mensajes de información de forma periódica o seguido a un evento de ruptura de enlace. Sin embargo, los mensajes no inundan la red sino que se intercambian únicamente entre vecinos locales. En la implementación de este protocolo, cada nodo almacena :

- Lista de vecinos
- Tabla con la topología (TT)
- Tabla con el próximo salto de la ruta
- Tabla de distancia al destino

En redes grandes, el tamaño de los mensajes intercambiados puede ser muy grande y el consumo de banda ancha importante. Por esas razones FSR utiliza diferentes frecuencias para el envío de esos mensajes. Las entradas correspondientes a nodos más cercanos son propagados con una frecuencia más alta. Mediante esa técnica, FSR funciona bien en redes de gran tamaño y mantiene el overhead bajo sin comprometer la exactitud de la computación de rutas cuando el destino está cerca. Cuando la movilidad de los nodos aumenta, las rutas hacia los destinos remotos se hacen menos exactas. Sin embargo, cuando un paquete se acerca a su destino, encuentra información

de encaminamiento más exacta. Como resultado, FSR es más útil para redes de gran tamaño donde la movilidad es alta y el ancho de banda bajo.

### 2.2.5. Protocolos multicast

#### MAODV

MAODV es la extensión multicast de AODV conocida también como Multicast AODV. Lo que se pretende construir son árboles multicast bidireccionales compartidos que conecten múltiples fuentes y destinos para cada grupo multicast. Estos árboles se mantienen mientras hay miembros del grupo conectados a alguna parte del árbol. Cada grupo multicast tiene un nodo líder, responsable de mantener el valor del número de secuencia. gracias a ese número de secuencia se consigue que el grupo multicast use siempre rutas actualizadas. El nodo líder es la raiz del árbol multicast. MAODV comparte muchas similitudes con el protocolo unicast AODV como son los paquetes de Route Request (RREQ) y Route Reply (RREP) así como la tabla de encaminamiento. Además se usan mensajes de Multicast Activations (MACT) y Group Hello (GRPH). El rango de diseminación de los RREQ lo indica el campo TTL de la cabecera.

Los nodos líderes de grupo inundan la red periódicamente anunciando su dirección y su situación de líder de grupo así como el número de secuencia del grupo. Cuando un nodo quiere enviar mensajes a dicho grupo multicast para el cual no conoce el líder, primero intenta hacerse líder del grupo. Si no recibe respuesta él mismo se convierte en líder y comienza a emitir. Si ya conocía la identidad del líder por haber recibido previamente un mensaje de anuncio, envía los mensajes de datos directamente al líder del grupo para que este los distribuya por el árbol multicast.

Cuando un nodo desea unirse a un grupo como receptor, envía una petición inundando la red. Estas peticiones pueden ser contestadas por cualquier miembro del grupo multicast. Las respuestas son enviadas al origen de modo que los nodos por los que pasa se convierten en nuevos miembros del árbol multicast.

### 2.2.6. Protocolos geocast

Aunque los protocolos geocast sean un caso particular de los multicast nos parece interesante detallar algunos de ellos debido al hecho de que son muy usados en redes VANETs. Los protocolos geocast son protocolos multicast dónde los grupos están organizados en funcción de la posición geográfica de los nodos de la red. Se usan protocolos geocast cuando se desea mandar un

mensajes a un grupo de vehículos de una determinada zona, para anunciar por ejemplo la presencia de un peligro en la carretera.

### LBM

*"Location Based Multicast"* [YKNHV 1999] es un protocolo orientado a la transmisión de datos que se basa en el protocolo unicast LAR, expuesto anteriormente. LBM se basa en un flooding tradicional salvo que los nodos tienen que decidir si retransmiten o no a los demás nodos según dos esquemas:

- LBM box
- LBM step

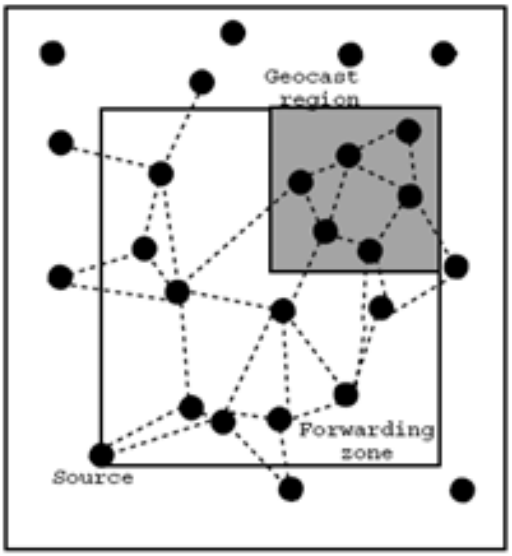



Figura 2.9: Esquema de LBM-box

Si el esquema considerado es LBM box, un nodo, a la recepción de un paquete geocast retransmite a los nodos que se encuentran el zona de forwarding, sino no reenvía el paquete. Según ese esquema la zona de forwarding es el rectángulo mínimo que engloba el origen del paquete geocast y la zona geocast, como se puede apreciar en la figura 2.9.

En cambio, en el esquema de LBM step se usa otra forma para determinar la zona de forwarding. Si A recibe un paquete geocast de un nodo B, A retransmite el paquete si está más cerca del centro de la zona geocast que B de por lo menos una distancia $\delta$. Este mecanismo se ilustra en la figura 2.10. Consideramos que $\delta = 0$. B reenviará el paquete recibido de A ya que $dist_A > dist_B$, dónde $dist_X$ es la distancia del nodo X al centro de la zona

geocast. Sin embargo, K descartará el paquete de B por estar más lejos del centro de la zona geocast. Resumiendo, este protocolo asegura que en cada retransmisión el paquete se acerca más a la zona geocast.

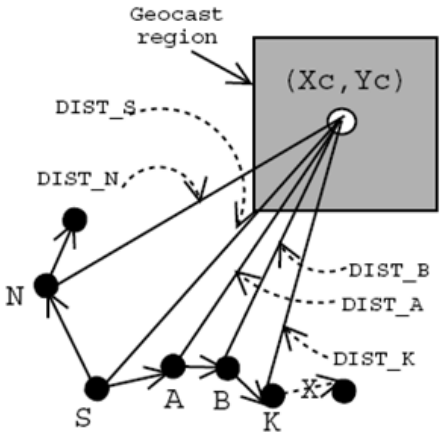



Figura 2.10: Esquema de LBM-step

### GEOTORA

GEOTORA como su propio nombre lo indica deriva directamente del algoritmo unicast TORA. Se construyó de la siguiente manera: se modificó TORA para hacer un protocolo anycast, modificando este protocolo anycast se consiguió un protocolo multicast. Veamos primero como funciona el algoritmo anycast.

En la versión unicast de TORA se asigna un DAG para cada nodo de la red. En cambio, en la versión anycast se asigna un DAG para todo el grupo anycast. Así se consigue que todos los nodos del grupo sean destino. En este caso, los enlaces entre nodos del grupo no tienen dirección ya que no nos interesa realizar encaminamiento dentro del grupo anycast, basta con alcanzar un nodo del grupo anycast.

El protocolo GEOTORA solo presenta una pequeña variación respeto a la versión anycast de TORA. Se mantiene un único DAG para todo el grupo geocast, logrando que cualquiera de los nodos presentes en la zona geocast sea destino. Primero, el protocolo realiza un anycast hacia un nodo de la zona geocast. A la recepción de un paquete de anycast, el nodo se encarga de retransmitir en modo flooding a todos los nodos de su zona geocast. Veamos un ejemplo con la figura 2.11. Si el nodo E quiere mandar paquetes a una zona geocast, reenvía el paquete por el enlace (E,G) al nodo G. A su vez el nodo G lo reenvía al nodo A, como este ya pertenece a la zona geocast, inicia el flooding limitado. Los nodos B y C al recibir el paquete de A reenvían el

paquete a sus vecinos. Cuando el nodo A recibe el pquete de B o C no reenvía el paquete ya que lo ha hecho previamente. De esta manera el paquete llega a todos los nodos de la región geocast.

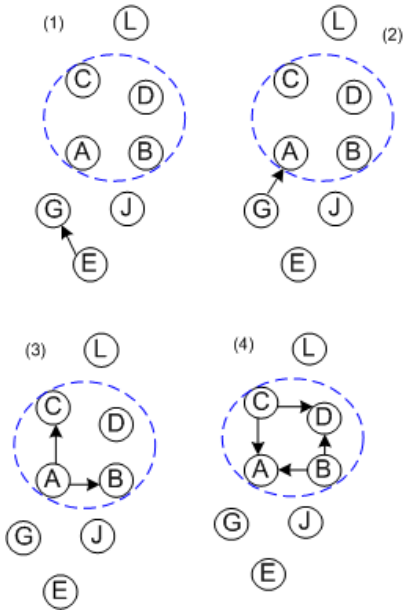



Figura 2.11: Funcionamiento de GEOTORA

### GEOGRID

GEOGRID [WLYTKLJS 2000] es un protocolo geocast derivado del unicast GRID. Al igual que GRID, GEOGRID realiza una partición del área geográfica que ocupa la red en celdas de dos dimensiones. Cada celda es un cuadrado de dimensiones $d \times d$. La zona de forwarding está definida por los nodos origenes y la zona geocast, de forma similar a la versión box de LBM. En cada celda, se elige un nodo gateway. La diferencia principal entre LBM y GEOGRID es que sólo los nodos gateways tienen la responsabilidad de transmitir los paquetes geocast. Existen dos versiones de GEOGRID: la versión basada en flooding y la versión basada en tickets.

En la versión basada en flooding, sólo los nodos gateways de la zona de forwarding transmiten los paquetes geocast. En la versión basada en tickets del protocolo, sigue siendo verdad que sólo los gateways retransmiten pero no todos. El origen distribuye (m +n) tickets para una zona geocast de $(m \times n)$ celdas a los nodos gateways de la zona de forwarding que están más cerca de la zona geocast. El gateway que recibe X tickets sigue el mismo metodo de distribución que el origen. En la figura 2.12 vemos que el nodo origen genera

5 tickets, 2 los entrega a A, 2 a B y 1 a C, que son los gateways más cercanos a la zona de geocast.

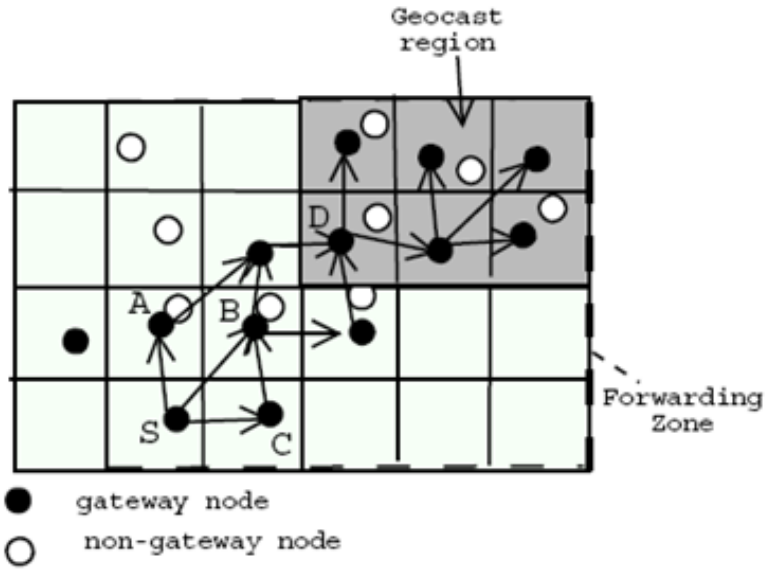



Figura 2.12: Esquema GEOGRID

Cada gateway transmite paquetes GATE que indica su naturaleza de gateway al resto de la red. Un nodo que quiere mandar tráfico geocast y que no tiene conocimiento de un gateway en su celda, manda un paquete BID para ofrecerse como gateway para esa celda. Un nodo que recibe un BID y que está más cerca del centro de la zona geocast manda a su vez un BID. El nodo que transmite el último BID (2 ms sin recepción de BID) en la celda se considera gateway para esa celda. Otra opción para elegir el gateway es elegir múltiples gateways temporales dentro de la misma celda. En esta situación si un gateway recibe un paquete de otro gateway más cercano al centro deja de ser gateway automáticamente sin enviar ningún mensaje de control explícito. Otra manera efectiva de elegir gateway se basa en el concepto de pesos, por ejemplo asignando a cada nodo un peso inversamente proporcional a su velocidad.

Además, cada gateway evalua cada 300 ms si ha quitado la celda. Si es el caso, el nodo manda un paquete RETIRE que inicia un nuevo proceso de elección de gateway en la celda.

### GAMER

*"Geocast Adaptative Mesh Environment for Routing"* (GAMER) es un protocolo geocast que se basa en la idea de crear rutas redundantes desde el

origen hacia una zona geocast. Esa idea proviene de la constatación que una sóla ruta hacia la zona geocast es frágil sobre todo en un entorno de movilidad muy alta, como es el entorno vehícular. Por eso, GAMER propone rutas redundantes basadas en mallas hacia una zona geocast.

Un nodo que desea transmitir un paquete geocast, primero manda mediante un flooding un paquete de JOIN-DEMAND. El flooding sigue en la zona de forwarding hasta alcanzar un nodo de la zona geocast. El nodo alcanzado de la zona geocast manda en sentido inverso unicast hacia el origen un paquete JOIN-TABLE. Cuando el nodo origen recibe la respuesta JOIN-TABLE puede empezar a mandar paquetes geocast a través de las mallas de la red.

GAMER se adapta de forma dinámica a la topología de red cambiando el tamaño de la zona de forwarding, lo que cambia la densidad de las mallas en tiempo real. Como consecuencia, cuando los nodos son de movilidad alta una malla densa se crea. En cambio, cuando baja la movilidad, la malla se hace menos densa. GAMER puede elehir entre tres esquemas de zonas de forwarding: CONE, CORRIDOR y FLOOD.

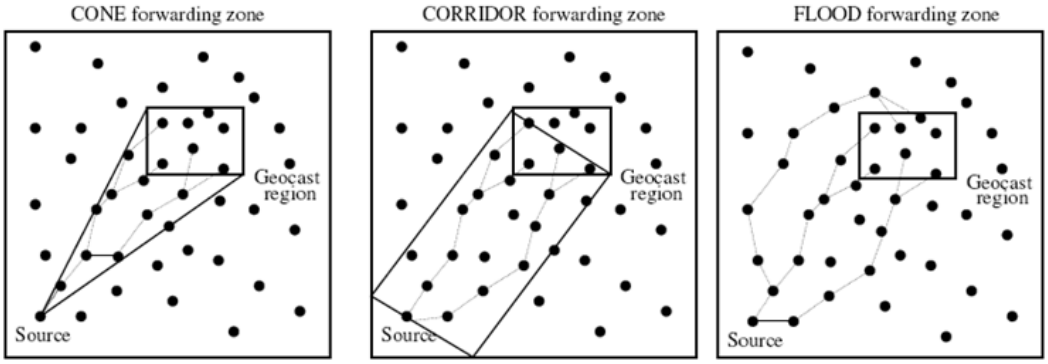



Figura 2.13: Zonas de forwarding GAMER

Los autores de GAMER proponen dos versiones del protocolo: una activa y otra pasiva. En la versión pasiva, se manda un paquete de JOIN-DEMAND a intervalos regulares sin consideración de si se ha recibido o no un JOIN-TABLE. En su versión activa GAMER establece igualmente unintervalo para mandar JOIN-DEMAND a la diferencia de que se adapta a los eventos de recepción de JOIN-TABLE. Si no se ha recibido un paquete JOIN-TABLE después de un tiempo conocido como SWITCH-TIMER se intensifica la frecuencia de envío de JOIN-DEMAND.

## 2.3. Seguridad

Los requisitos de seguridad en una VANET son los mismos que en una red tradicional, es decir:

- Confidencialidad: La información sólo debe ser legible por los autorizados.

- Integridad : La información sólo puede ser modificada por los autorizados.

- Disponibilidad: El sistema debe ser disponible cuando se necesita.

- No repudio: No se puede negar la autoría.

Sin embargo, todas las características de las VANETs que hemos descrito anteriormente (topología dinámica, falta de un procesamiento centralizado...etc.) hacen que sea mucho más díficil cumplir estos requisitos de seguridad. La política de seguridad a aplicar en un entorno ad-hoc dependerá, en gran media, de la aplicación y del escenario concreto para los que se realiza el despliegue de la red.

Las propuestas de seguridad se centran en aspectos concretos del problema. Se identifican cuatro aspectos clave que deberán ser cubiertos por cualquier política de seguridad en redes ad-hoc: control de acceso, sistema de detección de intrusos (SDI), seguridad de los protocolos de encaminamiento y servicios de gestión de claves.

### 2.3.1. Ataques en redes VANETs

Ataques básicos :

- Falsificación de la información : El atacante difunde información falsa o errónea para que afecte al resto de los vehículos

- Manipulación de la información del sensor: Modificar su posición, dirección, velocidad, etc. para escapar de ciertas responsabilidades por ejemplo al haber provocado un accidente.

- Denegación de servicio: utilizar un inhibidor de frecuencia para conseguir que un vehículo no reciba ninguna señal de su entorno en una cierta zona.

- Falsicación de identidad.

- Rastreado de vehículos: Seguir la pista de un vehículo infectándolo con algún virus que monitorice el estado de dicho vehículo.

Existen ataques sofisticados como el vehículo oculto o el túnel pero no los vamos a detallar en este documento.

### 2.3.2. Control de accesso

Como en las redes tradicionales, las VANETs necesitan un mecanismo que controle el acceso tanto a la red como a los servicios que provee. Las consequencias de un ataque en el cual un intruso tendría acceso a los servicios de la red pueden ser catastróficas ya en las VANETs los nodos asumen tareas de gestión y de encaminamiento al no tener una unidad de centralización. Un intruso podría desviar el tráfico durante el encaminamiento o tener acceso a claves de identificación.

En la capa de red, es necesario garantizar que ningún nodo no autorizado se una a la red bien para recibir información o para encaminarla. Así mismo a nivel de aplicación también es imprescindible asegurarse que elementos sin autorización no acceden a servicios, por ejemplo al servicio de gestión de claves.

El control de acceso consiste generalmente en la autenticación de los usuarios de la red. Es decir para acceder a la red y a sus servicios, un usuario debe identificarse de forma unívoca y la red lo autentica como autorizado para el acceso. En ciertas redes ad hoc los servicios se encuentran centralizados mientras que en otras están distribuidos, este hecho hace necesario el uso de diferentes mecanismos de control de acceso. Si elegimos un mecanismo de control de acceso distribuido para la red, será necesario un control de acceso basado en certificados digitales y autoridades certificadoras. En otros esquemas con servicios centralizados se requiere una autenticación basada en usuario y contraseña. Es muy útil hacer un estudio previo de las necesidades de seguridad de la red a desplegar, de esta forma, se podrán adecuar los mecanismos de control de acceso a la red.

### 2.3.3. Sistemas de detección de intrusos

El control de acceso consiste en una primera línea de defensa para impedir el acceso a la red a intrusos. Los sistemas de detección de intrusos (SDI) forman una segunda línea de protección muy importante.

Existen varias propuestas de SDI para VANETs, veamos las más interesantes:

En [YZWL 2000] los autores proponen una arquitectura distribuida y cooperativa para la detección de intrusos. En este sistema, cada nodo ejecuta un agente SDI que monitoriza las actividades locales al nodo. Si el SDI detecta una intrusión a partir de las trazas locales inicia un procedimiento de respuesta. Si se detecta una anomalía pero que no hay evidencias formales de la intrusión se usa un protocolo cooperativo con los vecinos para determinar si la intrusión tuvo lugar o no.

En [OKRG 2002] se propone un sistema distribuido basado en tecnología de agentes móviles. Un agente móvil se define como una entidad software autónoma, ligera y dinámicamente actualizable que atraviesa la red y se ejecuta sobre ciertos nodos. Este método es especialmente apropiado en el caso de las VANETs, dónde los recursos como el ancho de banda de los enlaces o la capacidad de los nodos pueden ser limitados. Las diferentes funciones del SDI se distribuyen entre diferentes tipos de agentes de forma que la carga introducida por el SDI se reparte de forma eficiente entre los nodos de la red.

En cualquier caso, el empleo de técnicas de SDI dependen siempre de la aplicación y del escenario concreto sobre el cual se ejecuta. Dada la sobrecarga que pueden introducir estos mecanismos, en términos de transmisión sobre el medio inalámbrico, de procesamiento y almacenamiento en los nodos, su uso puede resultar justificable únicamente en aplicaciones con fuertes requisitos de seguridad y en aquellas en las que los dispositivos involucrados dispongan de suficiente capacidad y autonomía como para que el SDI no imponga limitaciones intolerables para las prestaciones de los servicios finales ofrecidos al usuario.

### 2.3.4. Seguridad en el encaminamiento

Los nodos en una VANETs actúan como routers, participando en el protocolo de encaminamiento para descubrir y mantener rutas hacia otros nodos de la red. En las redes tradicionales, los routers son administrados por operadores de confianza pero eso deja de ser cierto en las VANETs dónde cada nodo que se une a la red participa en la toma de decisiones. Si el resultado del algoritmo de encaminamiento es manipulado, el funcionamiento normal de la VANET pueder verse seriamente afectado. Por este motivo la seguridad en el encaminamiento es de primera importancia para la seguridad global del sistema.

La investigación para proporcionar protocolos de encaminamiento seguros sigue hoy en día, ya se han propuesto algunos esquemas. Se ha definido un conjunto de técnicas para diseñar algoritmos de encaminamiento ad-hoc resistentes a intrusiones, este conjunto se llama TIARA. Varios protocolos se

basan en las técnicas TIARA como por ejemplo SRP o ARIADNE.

SRP proporciona información segura y autenticada a cada par de nodos que desea establecer una comunicación. El establecimiento se hará bajo una asociación de seguridad entre el nodo que inicia la comunicación y el nodo destino.

ARIADNE usa un proceso de criptografía simétrica que permite asegurar la integridad y la autenticación en las comunicaciones del protocolo.

### 2.3.5. Cifrado y gestión de claves

El empleo de técnicas de cifrado y de firmas digitales como mecanismo de seguridad requiere el uso de claves criptográficas, que serán compartida por todos los nodos. Por lo tanto, se debe disponer de un mecanismo seguro para la gestión de claves.

Se puede dividir las VANETs en dos grupos: las auto organizadas que se gestionan de forma autónoma y las VANETs que hacen uso de una entidad externa de confianza para la gestión de claves. En esquemas de VANETs pura, sin red de respaldo, es más apropiado usar un esquema de gestión de clave que no depende de ninguna entidad externa. En cambio, si se dispone de una red de respaldo, se puede optar por esquemas de tipos centralizados. Las soluciones las más populares son:
Para una red VANET pura:

- Gestión de claves en cadena de certificados.
- Gestión de clave basada en movilidad.

Para un red VANET híbrida:

- Autoridades de certifiación distribuidas.
- Gestión paralela de claves.

Existen muchas otras opciones muy interesantes, pero dado el alcance de este documento nos conformaremos con explicar las alternativas mencionadas.

#### Gestión de claves en cadena de certificados

Cada nodo genera su certificado, se distribuye y se almacena en cada nodo de la red. Si un nodo deja de fiarse de otro nodo, se puede pedir una renovación del certificado. Del mismo modo, si un nodo sospecha que su clave privada ha sido comprometida, puede revocar su propio certificado y generar otra clave privada.

### Gestión de claves basada en la movilidad

Se basa en un esquema de distribución peer-to-peer de las claves de los nodos basada en la movilidad de cada nodo. Se transmite una clave a un nodo según la movilidad que tiene en un momento para que este nodo distribuya las claves a los nodos a su alcance. Se rompe así la necesidad de tener una entidad externa para compartir las claves.

### Autoridades de certificación distribuidas

Se basa en una entidad externa de certificación que se encarga de distribuir las claves a los nodos de la red. Esta entidad debe ser altamente segura para que ningún atacante pueda tomar el control de ella y comprometer los mecanismos de certificación. Se puede distribuir los certificados de forma parcial o total.

En un mecanismo de distribución parcial de los certificados se elige un subconjunto de nodos llamados servidores a los cuales se transmiten las claves. Esos nodos deben disponer de una clave privada y una clave pública para que la entidad externa les pueda identificar de forma unívoca. Cada uno de los servidores genera una firma parcial utilizando su clave privada que es enviada a un combinador, que puede ser cualquier servidor. El combinador reconstruye así la firma digital.

En un mecanismo de distribución total de los certificados, la clave se distribuye a todos los nodos de la red y requiere que un nodo use la entidad externa para contactar con cualquier vecino. No es necesario el concepto de combinador ya que será el propio nodo quién reconstruye la firma digital del grupo.

### Gestión paralela de claves

Esta alternativa descrita en [SYRK 2004] se basa en una distribución parcial de los certificados por parte de una entidad externa y de un mecanismo de cadenas de certificados. La propuesta es conocida como *Composite Key Management*. La entidad externa distribuye el certificado a nodos servidores y luego tiene lugar el mecanismo de cadenas de certificados.

## 2.4. Servicios

Una plataforma de comunicaciones V2V y V2I permite el despliegue de multitud de servicios dirigidos a varios agentes como son el conductor, el resto de los ocupantes del vehículo, la administración, empresas, etc. Estos servicios ayudarán de forma inestimable en temas tan críticos como la seguridad en la conducción. Aunque una plataforma de comunicaciones en el

entorno vehícular permite desplegar una infinidad de servicios, en el presente apartado se mostrarán los más aceptados y los que pensamos que aportan las mejoras las más significativas a medio o largo plazo.

### 2.4.1. Sevicios para la seguridad vial

Los servicios dirigidos a la segurida vial son de forma clara los más importantes y los más criticos dado que su objetivo no es otro que salvar vidas disminuyendo el número de accidentes en la carretera. En este contexto se está haciendo un esfuerzo importante por parte de la comisión europea en la investigación, desarrollo e implementación de este tipo de servicios con el fin de que entren en actividad lo antes posible.

#### Mecanismos anti-colisión

Se trata de un servicio de ayuda a la conducción que sirve para detectar posibles obstáculos en la vía. La funcionalidad principal consiste en el aviso mediante señales acústicas al conductor de la presencia de otro vehículo o de que se acerca a una velocidad peligrosa para ese entorno. Este servicio requiere mucha rapidez a la hora de establecer el enlace y no es tan importante el tema de encaminamiento ya que básicamente la comunicación se dará entre vehículos con visión inálambrica directa sin nodos intermediarios.

Para un correcto despliegue sería necesaria una pequeña instalación en los equipos de los usuarios que enviase a sus vecinos información de posición, trayectoria y velocidad así como un mecanismo que permanentemente escuche la información enviada por el resto de los vehículos y la infraestructura.

#### Aviso de peligro

La funcionalidad principal de ese servicio consiste en detectar eventos peligrosos para informar al resto de los vehículos de la red. Los sensores pueden detectar un peligro y avisar al conductor con una breve descripción o el conductor mismo puede detectar el peligro y a través de una interfaz vocal describir el peligro para el resto de los usuarios.

Puede interesar mandar la información a todos los usuarios de la red para informar por ejemplo que se produce un atasco en un cierto punto de la carretera dónde están circulando. Por otro lado, se puede necesitar un envío geocast, por ejemplo si se detecta un vertido de aceite en una salida de la vía solo interesa mandarla a aquellos que van a tomar esa salida. Por lo tanto, es necesario que los vehículos soporten protocolos broadcast y geocast que no sobrecargen la red con mensajes de control para que la información llegue al destino de manera eficiente y rápida.

#### eCall

Se trata de una regularización de la Unión Europea (UE). Este futuro servicio consiste fundamentalmente en una llamada desde el vehículo a un número de emergencia en caso de accidente. El objetivo es el despliegue completo de este sistema en 2009.

En caso de accidente, el equipo embarcado transmite una llamada de urgencia al centro de recepción de llamadas más adecuado y envía al mismo tiempo,determinados datos sobre el vehículo (principalmente su localisazión precisa). El sistema se basa en el empleo del número de urgencia único europeo 112, que permitirá garantizar su interoperabilidad en toda la UE. La llamada de emergencia puede ser generada manualmente por los ocupantes del vehículo o automáticamente, en caso de accidente grave, mediante la activación de sensores instalados en el vehículo.

El principal requisito es la necesidad de comunicación, en cualquier lugar y bajo cualquier circunstancia, por lo que son imprescindibles tecnologías celulares con cobertura global en las vías.

El interés principal del servicio consiste en alertar de manera inmediata a los servicios de urgencias de localización exacta del accidente, lo que permitirá reducir considerablemente el tiempo de respuesta de dichos servicios. Según los estudios realizados, podría reducirse aproximadamente en un 50 % en las zonas rurales y en un 40 % en las zonas urbanas.

### 2.4.2. Servicios para la administración

#### Identificación de vehículos y obtención de información

Este servicio a largo plazo aportará una forma segura y ágil de recibir información de los vehículos sin necesidad de detenerlos. Será necesaria una legislación acorde que permita que todos los vehículos dispongan de la información necesaria en formato electrónico y que se transmita de manera automáticamente siempre que un dispositivo debidamente autorizado lo requiera.

Esto facilitará el control por parte de las autoridades para que todos los vehículos que circulen por vías públicas tengan en regla toda la documentación necesaria (permiso de circulación, seguro, tarjeta ITV...). Cuando se detecte una infracción el servicio podrá transmitir la consecuente denuncia de forma automática. Más a largo plazo aún, este servicio podría tener una extensión asociando también la identificación del conductor.

#### Detección de infracciones

Otro servicio desplegable gracias a una plataforma de comunicaciones V2I/V2V permitirá monitorizar los parámetros de de conducción de los vehículos. Gracias al sistema de posicionamiento y las comunicaciones, los elementos de infraestructura podrán obtener información sobre múltiples datos sensibles de ocasionar peligro, como son :

- Velocidades excesivas
- Tiempos de conducción sin parar
- Infracciones en semáforos y stops
- Transito por zonas prohibidas

### 2.4.3. Servicio de utilidad y entretenimiento

En este apartado descubriremos varios servicios con diferentes utilidades, calculo de rutas, comunicación vocal, entretenimiento, etc. Son servicios menos importantes que los relativos a la seguridad pero también aportan ventajas sobre los servicios tradicionales del sector automóvil.

#### Calculo óptimo de rutas con datos de tráfico en tiempo real

Este servicio puede ser usado tanto desde el propio vehículo como desde cualquier punto conectado a Internet. Podría ofrecerse como un servicio Web que permanentemente informa del estado de las carreteras en tiempo real. El hecho de que a largo plazo todos los vehículos puedan disponer de este sistema facilitará la identificación y recuento por parte de los equipos instalados en la infraestructura vial a tal efecto. Estos datos convenietemente recogidos y analizados servirán para mostrar el estado y preveer futuros atascos.

#### Tele diagnóstico y ayuda on-line en caso de avería

Este servicio se enmarca en las directivas de la comisión europea para liberar los manuales de reparación de los diferentes vehículos por parte de los fabricantes. Gracias a esta futura liberalización se podrán desplegar funcionalidades como:

- Consulta del manual electrónico y multimedia por parte del conductor desde el propio equipo embarcado.
- Consulta del manual por parte de las empresas de asistencia en carretera.

- Consulta a un sistema experto automático de datos en caso de avería.
- Envío automático de datos en caso de avería.
- Tele diagnóstico. Esta utilidad permite de forma remota valorar el grado de avería y en su caso facilitar la solución al conductor (instrucciones, envío de grua...)

**Acceso a Internet desde los vehículos**

Este servicio facilitará el acceso a Internet desde pantallas táctiles dentro de los vehículos. Enmarcado dentro del grupo de ocio y entretenimiento este servicio genérico suplirá posibles carencias en los contenidos del resto de los servicios. Los usuarios podrán acceder a toda la red e informarse de las condiciones meteorológicas del destino, reservar un hotel e incluso descargar contenidos.

Aunque podría ser tratado como un servicio aparte, una funcionalidad del acceso a Internet es la descarga y reproducción de contenidos multimedia. debido a su gran aceptación es previsible que a medio plazo gran cantidad de vehículos dispongan de medios para reproducir contenidos de video por lo que es razonable pensar que habrá una demanda de este tipo de servicios de descarga e incluso de Video On Demand.

Para ofrecer estos servicios el sistema de comunicaciones deberá ser capaz de acceder a Internet, bien a través de la red VANET o mediante tecnología móvil celular. Tanto la navegación como la descarga de correo electrónico no presentan grandes requisitos en términos de jitter, retardo y ancho de banda mientras que para el streaming de contenido multimedia es necesario unos buenos valores de calidad de servicio.

**Acceso a pasarelas para el paso de peajes**

Muchos de los problemas de retenciones en las autopistas y vías de pago se producen en los tramos de peaje, tanto en la entrada recogiendo el ticket como en la salida a la hora de pagar. Un servicio que gestionase esto de forma automática y evitase a los conductores el parar en estas zonas ahorraría tiempo a la vez que reduciría el coste para la empresa gestora de la vía.

Se ha pensado en un mecanismo mediante el cual los vehículos puedan asociar de forma segura su equipo a un medio estándar de pago, tipo tarjeta de crédito o moneder. Esta asociación permitiría el cargo automático del peaje de la vía sin necesidad de detener el vehículo.

El funcionamiento sería el siguiente: el usuario asocia su equipo embarcado a una pasarela de pago e indica los cargos permitidos para facturación inmediata. Una vez configurado el sistema, la próxima vez que se acerque a un punto de peaje el sistema instalado en el puesto se comunicará con el vehículo y preguntará si soporta este servicio, con la respuesta afirmativa por parte del vehículo y los datos de la forma de pago, se habilita el paso sin necesidad de detener el vehículo.

Este sistema aportará mejoras a los sistemas tradicionales de pago en peajes ya que por un lado, aumenta la distancia de comunicación y permite atravesar el peaje a mayores velocidades que las actuales.

Por supuesto la seguridad de este servicio debe estar garantizada para evitar posibles ataques y el uso fraudulente de las tarjetas de pago de los usuarios.

### Búsqueda y reserva de plazas de aparcamiento en el destino

Muchos de los parkings públicos ya disponen de un mecanismo informatizado que informa a los vehículos entrantes de la localización de las plazas libres. Este servicio deberá ser una extensión a este mecanismo de forma que los usuarios desde el propio vehículo y en ruta pueda comunicarse con el parking destino, notificarle la hora aproximada de llegada y reservar una de las plazas. El sistema del parking por su parte aceptará la petición, facturará el cargo (si procede) e indicará al usuario como llegar hasta su plaza.

### Información y alertas de gasolineras

A través de este servicio, los usuarios podrán interrogar al sistema de las distancias a las gasolineras más próximas, la empresa y las tarifas de los distintos carburantes. Para ello las diferentes gasolineras que lo deseen entregarán esta información y se comprometerán a tenerla actualizada en cada momento.

Una extensión de este servicio, a largo plazo será la integración de sensores en el equipo que informan de la cantidad de combustible restante y con la ruta programada informa al conductor la gasolinera recomendada para repostar.

### Envío de publicidad

Siempre contando con el permiso de los usuarios, se puede desplegar un servicio mediante el cual los equipos de la infraestructura envíen publicidad, básicamente relacionada con los servicios de la vía. Los usuarios podrían configurar sus equipos para aceptar o rechazar este tipo de publicidad incluso

definir un perfil con sus preferencias al respecto. Este perfil sería modificable dinámicamente de forma que al circular por autopista aceptara avisos de publicidad de restaurantes y gasolineras y, circulando por tramos urbanos, anuncios de parkings.

## 2.5. Calidad de servicio

El concepto de calidad de servicio (QoS) se utiliza para evaluar las prestaciones cuantitativas y cualitativas que se pueden ofrecer por una red a un servicio dado. los requisitos de calidad de servicio son:

- retardo extremo a extremo
- Ancho de banda disponible
- Probabilidad de pérdida de paquete
- Jitter

La llegada de nuevas aplicaciones de tiempo real como son el video streaming o el tráfico de voz por ejemplo, han hecho que la calidad de servicio de las redes se convierta en un requisito de primera importancia. Las redes móviles, debido a sus especiales características, hacen que la provisión de QoS sea un tema especialmente complicado. En este apartado se ofrece una revisión sobre el estado del arte de las QoS en redes ad-hoc. Se realizará un repaso de las principales iniciativas y se presentarán las líneas de trabajo que mayor viabilidad presentan en la actualidad.

### 2.5.1. Modelos de calidad de servicio

Las mayores propuestas de modelos de QoS son las estudiadas por el IETF a través de dos grupos de trabajo : Intserv (servicios integrados) y Diffserv (servicios diferenciados).

Intserv se basa en la idea de reserva de recursos en la red por flujos. Para cada flujo entrante se definen los recursos (ancho de banda, retardo, ...) que serán necesarios para este flujo. Cada nodo en el camino entre la fuente y el destino indica si puede asegurar la reserva y mantiene una tabla con el estado de reserva por flujo. La principal limitación de este modelo es la gran cantidad de información que se debe almacenar en cada nodo, provocando que la solución no sea aplicable en situaciones con gran cantidad de flujos entre usuarios finales.

Diffserv propone la agregación de flujos según la QoS, solucionando de esta forma los problemas de esalabilidad de Intserv. Diffserv define un campo de la cabecera IP, *Diffserv Code Point* (DSCP) asociado a la cabecera IP, de manera que el tratamiento de este tráfico en los nodos intermedios vendrá determinado por el valor asociado a este campo. De esta forma, se logra la agregación de flujos, consiguiendo un tratamiento especial para cada servicio en función del código DSCP.

### 2.5.2. Señalización para la reserva de recursos

Se necesita un mecanismo de señalización que se encargue de efectuar la reserva y la liberación de recursos en la red.

Uno de los mecanismos más extendidos es el protocolo RSVP, definido por el IETF. Se basa en la reserva de recursos extremo a extremo mediante los mensajes PATH y RESV que recorren el camino de una fuente hacia un destino estableciendo une reserva en los nodos intermedios. Sin embargo, este mecanismo no resulta tan eficiente en redes VANETs ya que introduce una sobrecarga importante y no se adapta muy bien a la topología altamente dinámica de estos tipos de red.

Para resolver este problema nace INSIGNIA, que propone incluir los mensajes de señalización en las cabeceras de los paquetes. Así, la cabecera indica si el paquete necesita recursos o si ya tiene la reserva hecha. En caso de que se trate de una petición, el paquete pasa a un módulo de decisión que analiza la red para saber si puede ofrecer los recursos necesarios. Se marca la decisión en la cabecera y el paquete es retransmitido.

### 2.5.3. Calidad de servicio ligada al encaminamiento

Un protocolo de encaminamiento que soporta QoS debe ser capaz de optimizar las rutas utilizadas en términos de ancho de banda, retardo, jitter...etc. Sin embargo, la topología dinámica de las VANETs hace muy complicada la evaluación de las prestaciones en una ruta.

A continuación se expone la propuesta CEDAR, *Core-Extraction Distributed Ad-hoc Routing*. Se trata de un protocolo de encaminamiento con soporte de QoS. En primer lugar la extracción de núcleo permite identificar un conjunto mínimo de nodos en la red que formarán parte del núcleo. Todo nodo debe formar parte del núcleo o ser vecino de un nodo del núcleo. CEDAR propone un algoritmo para la elección de los nodos que compondrán el núcleo, y define un proceso de pseudo-broadcast para el intercambio de información

entre los nodos del núcleo.

Otro de los pilares que componen CEDAR es la propagación del estado de enlace, cuyo objetivo es que cada nodo del núcleo conozca el estado y topología de los enlaces locales, así como los enlaces más lejanos pero estables y con gran ancho de banda.

El proceso de cálculo de ruta se realiza de la siguiente manera; cuando un nodo desea enviar información a un destino, previamente manda un mensaje indicando origen, destino y ancho de banda solicitado. Esta información se propaga por el núcleo a través del pseudo-broadcast, hasta que alcanza el destino, mientras los nodos intermedios comprueban la disponibilidad de ancho de banda en cada salto.

# Capítulo 3

# Especificación de escenarios

En este apartado se detallan los estudios de simulación que se quieren realizar. Entendemos por estudio de simulación los escenarios aplicados a las topologías de red descritas en el primer capítulo. Para cada escenario definido se obtendrán datos para ambas topologías (circuito urbano y autopista) con los diferentes perfiles de tráfico para cada una de las topologías (alto, medio y bajo).

Para cada caso se harán dos pruebas (salvo que se indique de otra forma en la especificación de escenarios) : una usando conexiones TCP y otra usando conexiones UDP,que son los dos protocolos de comunicación los más usados por los servicios corrientes en la actualidad. Las aplicaciones usando esos protocolos deben ser fáciles de simular, por lo tanto hemos elegido FTP sobre TCP y CBR sobre UDP.

## 3.1. Escenarios

### 3.1.1. Escenario 1: VANET pura

Este escanario debe permitir similar una situación clásica en redes VANETs, es decir una comunicación inalámbrica entre dos vehículos en modo ad-hoc, sin infraestructura ni red de respaldo. Dado que la comunicación es directa y no implica nodos intermedios, el rendimiento de esta comunicación sólo va a depender del esquema de movilidad y de la tecnología inalámbrica considerada. En nuestro caso, y en espera del estándar 802.11p, usaremos la tecnología inalámbrica 802.11b para las comunicaciones vehiculares. Por lo cual, con la tecnología fijada, este escanario nos permite tener una comparación de los efectos de los esquemas de movilidad en las comunicaciones, viendo como influyen en los rendimientos de red.

El escenario es el siguiente:se establecerá una comunicación desde un nodo origen cuando el destino se encuentra a su alcance, mientras que si la distancia de separación es mayor que dicho radio, la comunicación se cortará.

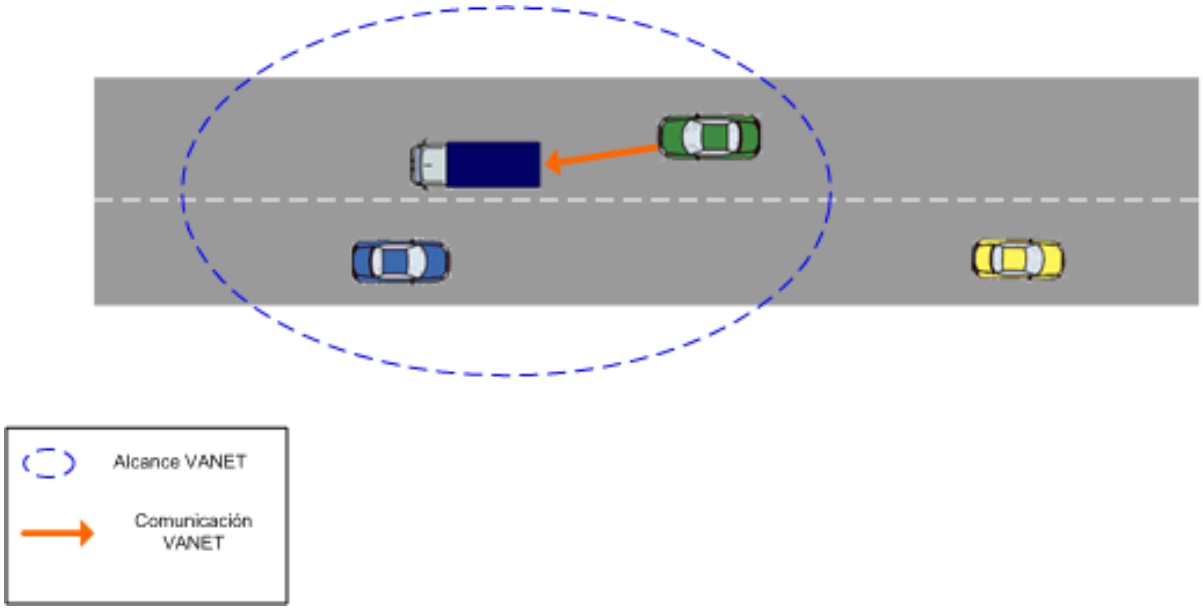



Figura 3.1: Escenario de comunicaciones VANET puras

### 3.1.2. Escenario 2: Comunicación VANETs pura a través de nodos intermedios

Este esceanrio nos permitirá obtener una comparación de diferentes protocolos de encaminamiento unicast. Existen muchos estudios que se proponen comparar protocolos de encaminamiento cuando el número de conexiones entre les vehículos se multiplica. En este trabajo nos centramos en la influencia de la topología de red para cada uno de los protocolos considerados. Por lo cual, elegimos dos nodos para las comunicaciones. Estos nodos deben ser elegidos con cuidado ya que deben ser representativos de las diferentes densidades de cada topología y densidades de tráfico. Se deben elegir nodos que en las diferentes topologías mantengan la misma trayectoria en el tiempo y lo único que cambie de una densidad a otra es el número de nodos que se encuentra entre ambos vehículos a lo largo de la simulación.

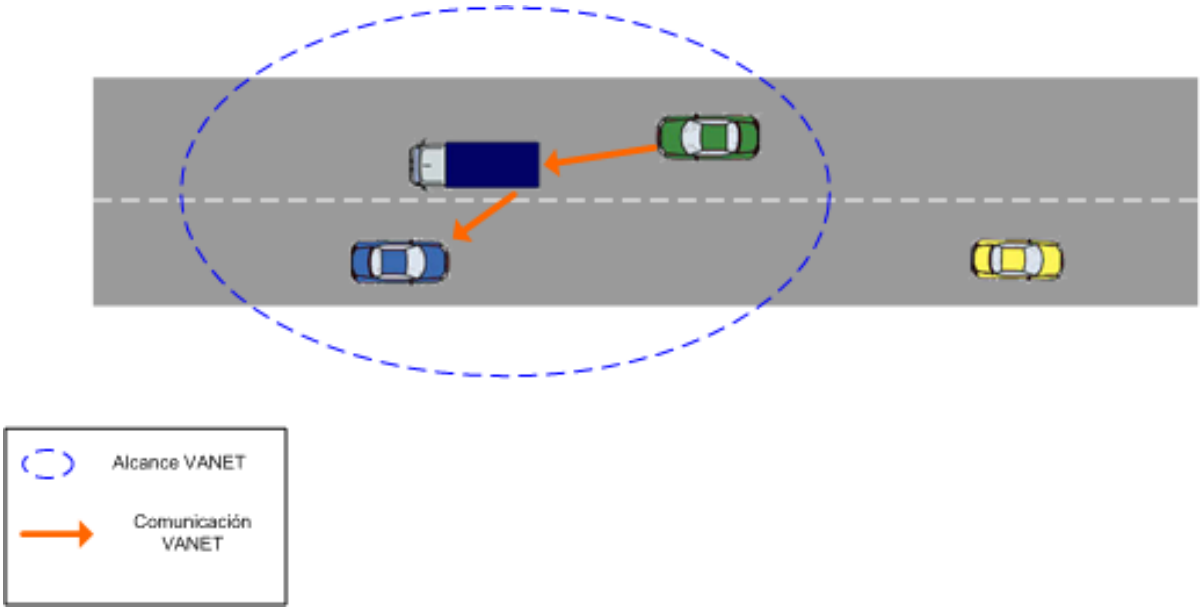



Figura 3.2: Escenario de comunicaciones VANET puras con nodos intermedios

### 3.1.3. Escenario 3: Comunicación entre dos vehículos con red de respaldo UMTS

Cada nodo dispone de dos interfaces: una principal que se conecta a través de 802.11b y otra de respaldo que se conecta por la red de respaldo UMTS.

Siguiendo nuestra línea de trabajo, fijaremos dos vehículos para las comunicaciones. Por defecto, las comunicaciones se establecerán por la VANET, de forma similar a los dos primeros escenarios. Si el nodo origen y destino pueden comunicarse entre sí , la comunicación se hará por la VANET de forma similar al escenario 1. Si por el contrario, el nodo destino no es alcanzable a través de la VANET, por la razón que sea, la comunicación se hará sobre el enlace de respaldo basado en UMTS. Se monitoriza el enlace para que en cuanto vuelva a estar disponible el enlace VANET, se vuelva a mandar tráfico por esa vía.

Sólo se manda tráfico UMTS desde el origen, es decir si un nodo intermediario detecta un fallo en un enlace de la VANET, no se enviará por la red de respaldo UMTS sino que seguirá los procedimientos habituales del protocolo original (buffer, descartar, etc.)

En este escenario se utilizará el protocolo que mejor resultado habrá dado en los escanarios anteriores. De esta forma, obtendremos una comparativa

que nos indicará si introducir una red de respaldo mejora las comunicaciones VANETs de forma significativa.

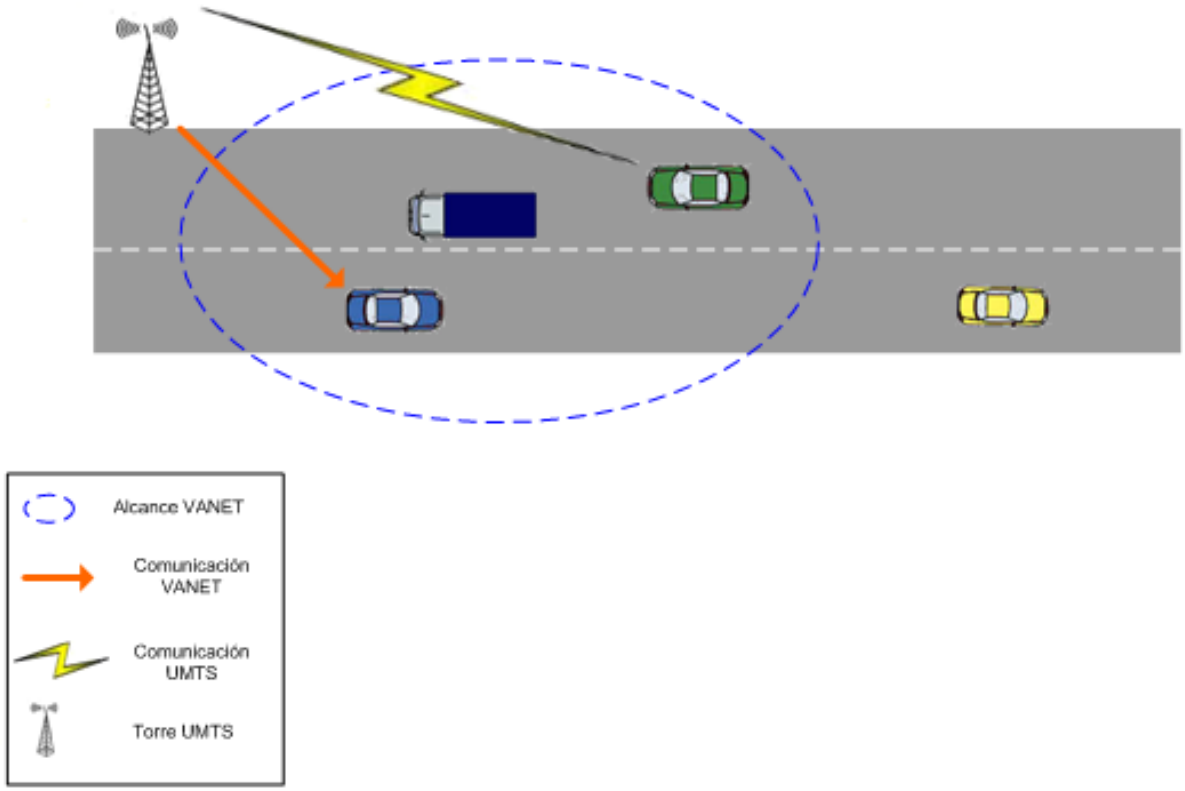



Figura 3.3: Escenario de comunicaciones VANET con respaldo UMTS

### 3.1.4. Escenario 4: Comunicación entre un vehículo y la infraestructura vial

Este estudio ilustra el concepto de comunicaciones V2I, es decir entre los vehículos y la infraestructura vial. En situaciones reales, la infraestructura vial se compone de los gateways colocados en paneles de señalización, en semáforos. Para simular la infraestructura vial, consideraremos nodos estáticos situados en lugares plausibles, como por ejemplo en los bordes de la carretera.

Este estudio nos permitirá establecer una comparativa de los protocolos geocast. Los nodos de infraestructura se encargarán de mandar tráfico UDP a todos los nodos de una determinada zona geográfica.

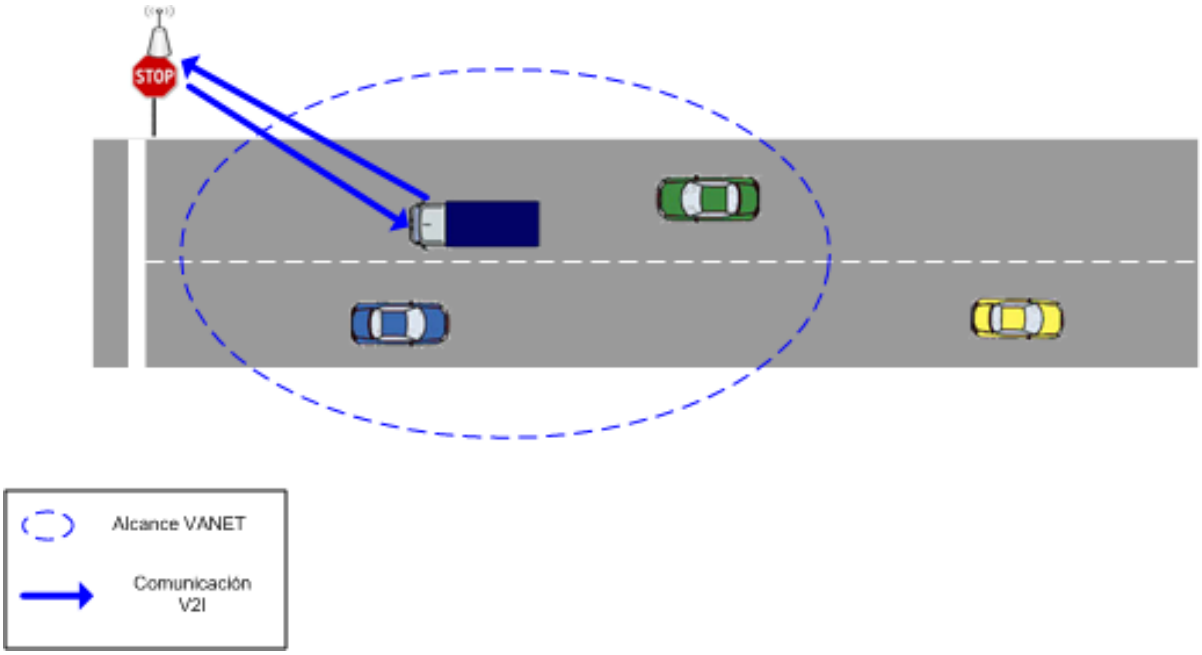



Figura 3.4: Escenario de comunicaciones V2I

## 3.2. Indicadores de rendimiento de red

Los indicadores son las medidas de rendimiento de red que nos permitirán comparar de forma cuantitativa los rendimientos de los protocolos en cada estudio.

### 3.2.1. Protocolos unicast

Para medir la eficiencia de los protocolos vamos a estudiar cuatro indicadores:

- Porcentaje de éxito (*Packet Delivery Fraction (pdfr)*): Es el porcentaje de paquete enviados que llegan al destino. Un paquete enviado se puede perder bien porque el retardo de transmisión es tal que no llega a tiempo y se considera como pérdido, o bien porque se ha dañado y los mecanimos de control del destino lo rechazan. El pdfr es un buen indicador para obtener una comparativa relativa a las tasas de pérdidas para cada protocolo. Un protocolo con tasas de pérdida altas no es satisfactorio ya que los rendimientos de red empeoran.

- Througput: Se mide la cantidad de datos digitales enviados al nodo destino, generalmente en paquetes por segundos o bits por segundos. Este dato tiene sentido únicamente en conexiones TCP ya que con

conexiones UDP no se preocupa de saber si un paquete ha llegado o no al destino.

- Retardo extremo a extremo: Queremos medir el retardo de transmisión, es decir el lapso necesario para que un paquete viaje de la fuente al destino. Es importante considerar el retardo por varios motivos. Por un lado, el retardo define la velocidad global de una red por lo cual nos da indicaciones de rendimientos importantes. Por otro lado, algunos servicios no pueden soportar retardos muy elevados, como los servicios de tiempo real por ejemplo, que necesitan calidad de servicio. Por lo cual, la medida del retardo extremo a extremo para cada protocolo de encaminamiento es una medida importante para la comparativa.

- Overhead: Son los paquetes de control generados por cada protocolo. Este indicador es extremadamente importante, sobre todo en nuestro caso dónde tratamos con protocolos de encaminamiento. Es obvio que un protocolo de encaminamiento introduce overhead al ser un mecanismo de control. Sin embargo, un protocolo que introduce una sobrecarga excesiva para su funcionamiento influye de forma muy negativa sobre el rendimiento de la red, ya que para mandar un paquete de datos útiles, se tendrá que mandar más paquetes de control, consumiendo precioso ancho de banda.

### 3.2.2. Protocolos geocast

Un protocolo geocast manda datos a los nodos de una zona geográfica que en ciertos casos pueden ser múltiples. Por lo cual, el estudio de los indicadores no se puede abordar de la misma manera. Por ejemplo medir el retardo extremo a extremo como lo hemos abordado en protocolos unicast no es una medida apropiada para los protocolos geocast, los enlaces hacia cada nodos son variables y los retardos de transmisión varian en consecuencia. Para nuestras simulaciones vamos a considerar cuatro indicadores.

- One Success Rate (OSR): Este indicador corresponde al porcentaje de éxito, es decir el porcentaje de paquetes que llega a un nodo de la zona geocast. Es una medida que permite aproximar el porcentaje de éxito para todos los nodos de la zona geocast, ya que está demostrado que el porcentaje de éxito para un determinado nodo destino es muy similar al OSR para todos los nodos de la zona.

- Paquetes totales por éxito: Es en valor absoluto el número de paquetes totales, útiles y de control, que genera cada protocolo para enviar la información a la zona geocast. Nos permite comparar el overhead introducido en la red para cada protocolo.

- Retardo extremo a extremo: Retardo de transmisión entre el origen del flujo geocast y un nodo destino. De la misma manera que anteriormente aproximamos esa medida al retardo extremo a extremo en la red.

- Número de saltos: esa medida nos da indicaciones relativas a la optimización del protocolo de encaminamiento; un protocolo es más eficiente si usa rutas óptimas (con menor número de saltos).

# Capítulo 4

# Plataforma de simulación

Siguiendo los requisitos de la plataforma de simulación se ha elegido un conjunto de programas de libre distribución y de código abierto. La base de la plataforma es el simulador ns2 (*Network Simulator*) [W2]. Esta elección se ha hecho considerando la amplia aceptación que recibe entre los grupos de trabajo para desarrollo de protocolos en redes MANETs. El hecho de que un programa sea muy utilizado es una ventaja porque dispondrá de numerosas implementaciones de protocolos, documentación y forums de usuarios.

Ns2 genera trazas de una simulación muy completas que nos permiten extraer la totalidad de las medidas de los indicadores elegidos para la comparativa.

Junto a ns2, usaremos un animador gráfico llamado nam, [W3]. Nam no aporta datos cualitativos a la simulación. Sin embargo, puede ser interesante poder visualizar de manera más visual los flujos de datos y los movimientos de vehículos, para poder detectar por ejemplo las pérdidas de paquetes.

Luego, para poder crear los patrones de movimientos que vamos a aplicar a los vehículos, utilizaremos programas llamados SUMO y MOVE. Gracias a ellos obtendremos las trazas de los patrones de movimientos a aplicar para cada estudio.

En este cápitulo describimos los programas utilizados, la instalación y el funcionamiento de la plataforma de simulación.

## 4.1. Componientes Software de la plataforma de simulación

Como lo hemos descrito antes, la plataforma de simulación se divide en cuatro bloques software de código abierto. A continuación, se describe en detalle cada uno de esos bloques:

### 4.1.1. Ns2

Ns2 es el corazón de nuestra plataforma de simulación. Probablemente se trata del simulador de red lo más extendido tanto en ambito de investigación como para objetivos docentes. Es un simulador de tiempo discreto cuya elaboración se inició en 1989 con el desarrollo de REAL *Network Simulator*. Una de las principales razones que lo hacen tan popular es el hecho de que la distribución posee licencia GPL, condición que impulsa el desarrollo libre del mismo.

#### Funcionamiento

Ns2 es capaz de simular las diferentes capas OSI (física, MAC, enlace, IP, transporte, aplicación) pudiendo modificar las caracteristicas de cada una de ellas.

Ns2 se apoya en dos lenguajes de programación para su correcto funcionamiento. Por un lado, el usuario introduce las especificaciones del escenario a simular a través del lenguaje OTcl, versión extendida de Tcl. Por otro lado, la implementación de los protocolos se escribe en C++.

Ns2 registra cada paquete de datos que atraviesa la red junto a sus características principales como por ejemplo, el instante de recepción, el número de secuencia, el tipo de paquete, etc. Estos parámetros forman la traza como resultado del procedimiento de ns2.

#### Secuencia de ejecución

A la hora de abordar la simulación de un protocolo en ns2, es necesario seguir los siguientes pasos:

- Implementación del protocolo a analizar mediante la incorporación de código C++ y OTcl dentro del núcleo de Ns2. Este paso no es necesario si se desea usar protocolos ya propuesto por Ns2. Ns2 cuenta con muchos protocolos ya implementados en su versión descargable (AODV, TORA, DSDV, DSR, por ejemplo). Pero puede ser necesario añadir la implementación de nuevos protocolos.

- Descripción de la simulación mediante OTcl. Se trata de definir el escenario a simular.

- Ejecución de la simulación. Se lanza el simulador proporcionandóle el fichero de descripción de simulación previamente definido.

- Existen múltiples formas de analizar los resultados de la simulación. En primer lugar, para visualizar la ejecución se puede usar el animador

gráfico de ns2, nam. Pero no nos proporciona los datos cuantitativos necesarios a un estudio riguroso.
Es posible extraer medidas cuantitativas a partir de los ficheros de traza que aporta la simulación. Se realiza un post-procesado que nos permite extraer medidas de indicadores de rendimiento de red, mediante un programa de tratamiento. En nuestro caso, hemos desarrollado en Java ese tratamiento post-simulación.

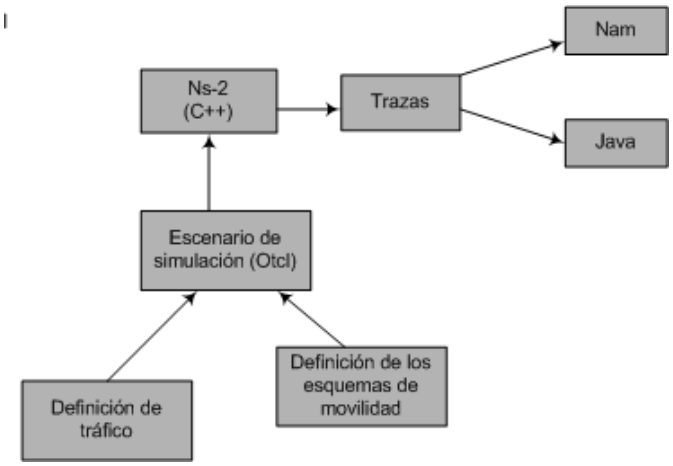



Figura 4.1: Esquema de módulos Ns2

Ns2 podría valernos para simular tráfico y obteber las trazas de comunicaciones. Sin embargo, para definir las carreteras y los patrones de movimiento es más comodo usar programas con interfaz gráfica que programar directamente en oTcl. Por esas razones usamos SUMO y MOVE.

### 4.1.2. MObility model generator for VEhicular networks (MOVE)

Esta herramienta [W4] permite crear mapas de carreteras urbanas o interurbanas (incluso se puede importar mapas reales). Nos permite crear también flujos de tráfico controlados, implementar semáforos, etc... Ha sido desarrollada por la *School of Computer Science and Engineering* de la Universidad *New South Wales* de Australia en Java.

La primera cosa que debemos hacer es crear un mapa, definiendo nodos y carreteras. Se hace de manera muy intuitiva a través de la interfaz gráfica de usuario.

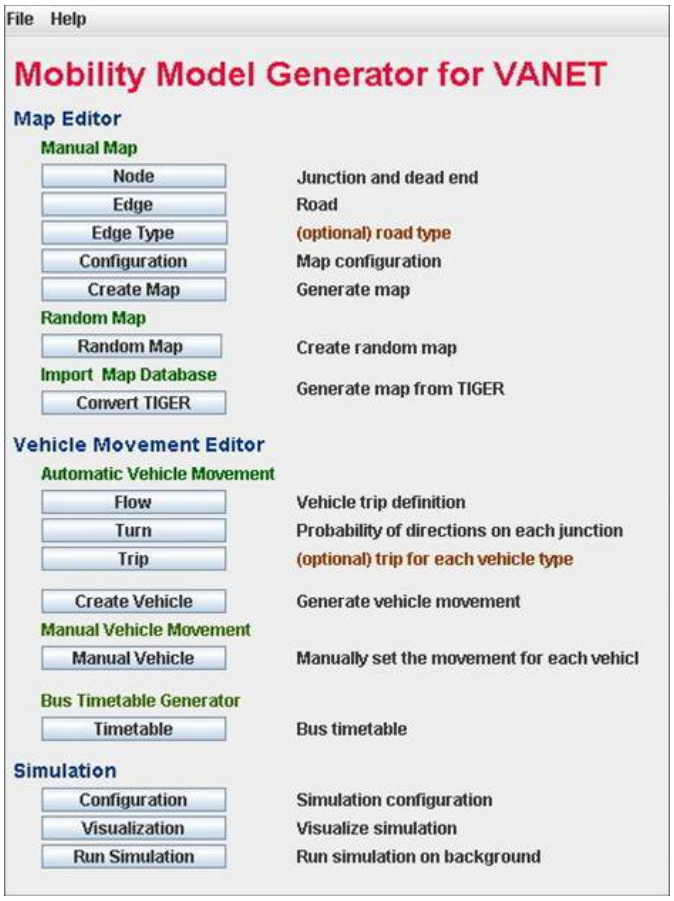



Figura 4.2: Menu del MOVE

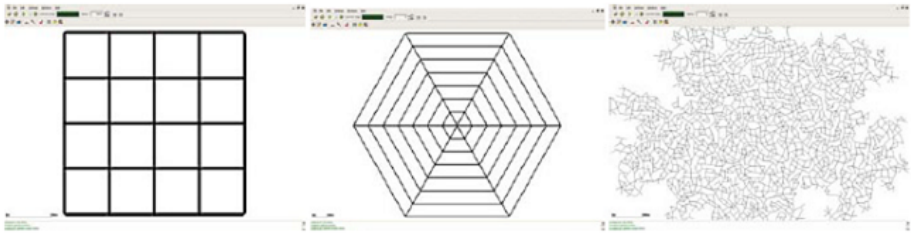


Figura 4.3: Mapas generados por MOVE

### 4.1.3. Simulation for Urban mobility (SUMO)

SUMO [W5] es un paquete de simulación de tráfico vial de código abierto. Esta herramienta se usa a través de MOVE para simular tráfico rodado con gran precisión, permitiendo desplegar la mayoría de los elementos que componen una vía, como semáforos, stops, carreteras de varios carriles, rotondas, etc. Es la herramienta encargada de generar el patrón de movimiento de los vehículos en las diferentes topologías para poder ser usado por el simulador ns2.

### 4.1.4. Tracegraph y Parse Java

Las trazas generadas por ns2 proporcionan toda la información sobre la simulación pero su complejo formato hace difícil la extracción de resultados de forma manual. Por esto se utilizan programas capaces de obtener los principales parámetros de rendimiento de red como el jitter, retardos... y mostrarlos de forma gráfica.

Para conseguir gráficos se ha usado el programa Tracegraph [W6].TraceGraph es una herramienta de código libre y que permite convertir trazas ns2 en gráficas.

Para extraer de manera cuantitativa los valores de la simulación hemos desarrollado en código Java un parse que reciben en entrada un fichero de trazas y devuelven los indicadores asociados a la simulación.

## 4.2. Procesos de simulación

1. Generación del mapa de carretera con MOVE. Inicialmente hay que definir las carreteras proporcionando las coordenadas de origen, destino, número de carriles, velocidad máxima de la vía, prioridad y extensión. También existen las opciones de importar mapas en el formato TIGER o crearlos de forma aleatoria, en cuadrículo o grid.

2. Creación de los flujos de vehículos con MOVE. Se definen los movimientos de tráfico, carretera inicial, carretera final, número de vehículos y tiempo durante el cual transcurren los movimientos. Existen opciones para especificar manualmente el movimiento de los vehículos proporcionando las carreteras por las que viaja, el tiempo, acelaraciones, deceleraciones, velocidades máximas, etc. También se pueden definir recorridos de autobuses y sus horarios habituales.

3. Simulación de tráfico con SUMO. Consiste en ejecutar la simulación de tráfico vial con el mapa y las condiciones de tráfico definidas anteriormente. El simulador SUMO mostrará de forma gráfica el comportamiento de los vehículos de modo que podremos visualizar si corresponde

con lo esperado. A la vez que se ejecuta la simulación se crea un fichero con las trazas de movimiento de los vehículos que será utilizado por el simulador ns2.

4. Simulación de red con ns2. Usando el patrón de movimiento creado en el paso anterior se define conexiones entre los diferentes vehículos. Es necesario crear un script de ns2 que defina las tecnologías radio a utilizar, el tipo de antena, el modelo de propagación, algoritmo de encaminamiento a simular, protocolo de transporte, etc. Con el script creado se ejecuta la simulación obteniendo dos trazas; una interpretable por el animador gráfico nam y otro con las trazas *wireless* que produce el simulador.

5. Análisis de los resultados. Gracias a Tracegraph y a nuestro programa Java que procesa las trazas y extrae datos significativos de la simulación podemos comparar y analizar los resultados de las diferentes simulaciones. Al cabo de ese paso se pretende concluir sobre el carácter óptimo de un protocolo en cada escenario.

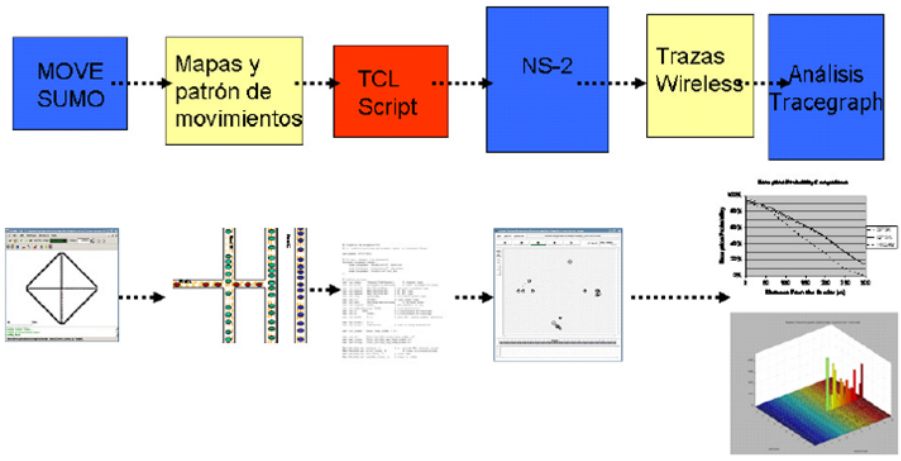



Figura 4.4: Proceso de simulación

## 4.3. Instalación de la plataforma

A continuación se muestra como instalar la plataforma de simulación paso a paso. Se parte de una máquina con Debian Sarge instalado Java SDK 1.4.2 o superior y disponiendo de un entorno gráfico.

### 4.3.1. ns2

El corazón de la plataforma de simulación es sin ninguna duda el simulador de red ns2 y su animador gráfico nam. Como todas las herramientas de la plataforma se trata de código abierto por lo que se puede descargar de forma gratuita de la página oficial: http://www.isi.edu/nsnam/.

#### Librerías

Además del propio código del simulador son necesarias las librerías de *tcl, tk, otcl, tclcl* pero recientemente se ha preparado un paquete que instala todas las dependencias. En nuestro caso se ha utilizado el paquete *ns-allinone-2.32.tar.gz*.

Además, el sistema en el cual vamos a implementar ns2 debe disponer de librerías de sistema para que la aplicación se instale de forma correcta. Por lo cual, antes de proceder a la instalación se ejecuta el siguiente comando:

```
# sudo apt-get install build-essential
# sudo apt-get install tcl8.4 tcl8.4-dev tk8.4 tk8.4-dev
# sudo apt-get install libxmu-dev libxmu-headers
```

#### Instalación

Una vez descargado simplemente hay que descomprimirlo y desde el directorio principal ejecutar:

```
./install
```

Una vez instalado, el propio programa da las instrucciones para terminar de configurarlo, básicamente se trata de trata de añadir al path los directorios dónde se encuentran los ejecutables de ns y las librerías tcl y tk y exportar dos variables más:

```
export LD_LIBRARY_PATH=/home/helene/ns2/ns-allinone-2.32/otcl-
1.11/:/home/helene/ns2/ns-allinone-2.32/lib
export TCL_LIBRARY=/home/helene/ns2/ns2-allinone-
2.32/tcl8.4.15/library
```

Esto sería suficiente para empezar a utilizar el simulador y su animador, para comprobar que la instalación se ha realizado de forma correcta existe una serie de validaciones y demostradores accesible desde el repertorio principal a través del comando:

```
./validate
```

### 4.3.2. SUMO

Como ya se ha adelantado, SUMO es un paquete de simulación de tráfico vial de código abierto. Se puede descargar desde: http://sumo.sourceforge.net. Para nuestro proyecto se ha descargado las últimas versiones estables del programa y de las librerías necesarias.

#### Librerías

Lo primero que tenemos que hacer es preparar nuestro sistema a la instalación de SUMO; se deben instalar las siguientes librerías:

```
# sudo apt-get update
# sudo apt-get install build-essential
# sudo apt-get install xorg-dev
# sudo apt-get install python
# sudo apt-get install python-dev
# sudo apt-get install libxext-dev
# sudo apt-get install libx11-dev
# sudo apt-get install freeglut3 freeglut3-dev libglut3
libglut3-dev
# sudo apt-get install libgl1-mesa libgl1-mesa-dev
# sudo apt-get install libjpeg62-dev libgtk2.0-dev
# sudo apt-get install libxxf86vm-dev libbz2-dev
# sudo apt-get install libglu1-mesa-dev
# sudo apt-get install mesa-common-dev xlibmesa-glu libgludev
libsdlm-dev xlibmesa-gl-dev libartsc0 libartsc0-dev
```

A parte de las librerías del sistema se debe instalar las librerías necesarias a SUMO: fox, gdal, proj y xerces. La página de SUMO nos proporciona los enlaces hacia las páginas de descargas de estas librerías.

```
 export PLATAFORMA=/home/helene/plataforma_sim/sumo
tar xzf fox-1.4.35.tar.gz
cd fox-1.4.35
./configure -with-opengl=yes -prefix=$PLATAFORMA && make
install
cd ..
tar xzf gdal-1.3.2.tar.gz
```

```
cd gdal-1.3.2
./configure -prefix=$PLATAFORMA && make install
cd ..
tar xzf proj-4.5.0.tar.gz
cd proj-4.5.0
./configure -prefix=$PLATAFORMA && make install
cd ..
tar xzf xerces-c-current.tar.gz
export XERCESCROOT=$HOME/xerces-c-src_2_7_0
cd $XERCESCROOT/src/xercesc
autoconf
./runConfigure -plinux -cgcc -xg++ -minmem -nsocket -tnative
-rpthread -P$PLATAFORMA
make
make install
```

**Instalando SUMO:**

```
 tar xzf sumo-src-0.9.8.tar.gz
cd sumo-0.9.8
./configure -with-fox=$PLATAFORMA -with-proj-gdal=$PLATAFORMA
-with-xerces=$PLATAFORMA -prefix=$PLATAFORMA
make install
```

### 4.3.3. MOVE

MOVE está desarrollado en Java y se puede descargar tanto el código como la documentación desde: http://www.csie.ncku.edu.tw/~klan/move/ Una vez descomprimido el paquete se comila desde el repertorio principal:

```
javac *.java
```

Para empezar a trabajar con MOVE basta con escribir desde el repertorio principal:

```
java vanetsim
```

## 4.4. Modificaciones al código de ns2

### 4.4.1. Protocolos geocast

La finalidad de los protocolos geocast es enviar información desde un nodo a todos los nodos que se encuentran en una determinada zona geocast. Para

utilizar estos protocolos debemos realizar algunos cambios al código del ns2. Se modifican los ficheros Makefile.in, packet.h, cmu-trace.cc, cmu-trace.h, god.h, goc.cc, ll.cc (ver apendices).

### 4.4.2. Respaldo UMTS

Deseamos simular una plataforma de comunicaciones híbrida compuesta por la red VANET y un enlace de respaldo UMTS o cualquier otra tecnología celular capaz de proporcionar ancho de banda suficiente. El funcionamiento será el típico de una VANET siempre que el nodo origen y destino puedan comunicarse entre sí, en el momento que no haya comunicación ad-hoc el nodo origen enviará la información a través del enlace de respaldo pasando por la infraestructura de la operadora móvil. Se tendrá que implementar un protocolo en ns2 que nos permita simular este comportamiento.

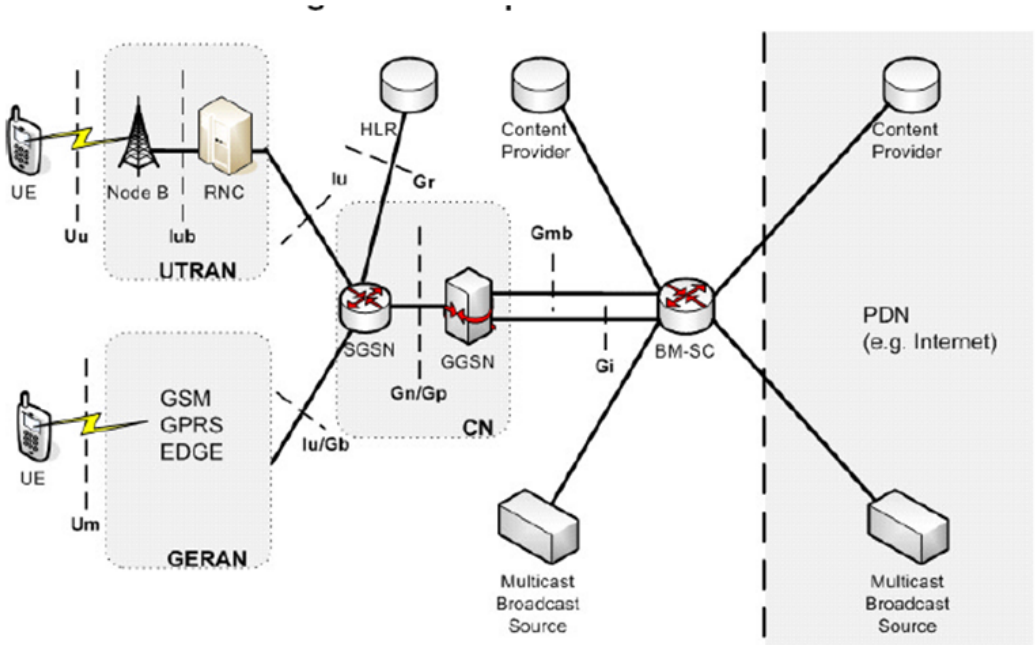



Figura 4.5: Arquitectura UMTS

Existe una implementación de UMTS para ns2, llamada EURANE [W9] desarrollada por el proyecto SEACORN. Esta implementación de UMTS para ns2 cubre muy bien los aspectos internos de la propia red, simulando con gran detalles el comportamiento de los distintos elementos: UE, Node B, RNC, SGSN, GGSN así como los distintos enlaces entre ellos.

Sin embargo, EURANE no permite simular la comunicación directa entre dos clientes (UEs) controlados por la misma RNC, debido a esta limitación se decide utilizar un mecanismo diferente para conseguir la comunicación UMTS dejando al margen la extensión EURANE.

Además ns2 no permite definir dos interfaces para un mismo nodo, hay que instalar una nueva extensión ; Enhanced NS (TeNs). Esta extensión es relativamente sencilla de implementar siempre y cuando se dispone de la version original entragada en la distribución, pero una vez que se ha modificado ns2, como es nuestro caso, la instalación se complica enormemente pudiendo provocar el funcionamiento erróneo del simulador.

Por estos motivos principalmente y dado que el resultado será prácticamente igual se ha decidido darle un nuevo enfoque al esquema de funcionamiento con dos interfaces AODV y UMTS. Se modificará el código del propio AODV para ns2 de forma que cuando dicho protocolo no sea capaz de mandar paquetes al destino, enviará un nuevo tipo de paquete especial. A la hora de analizar las trazas con nuestro parse Java, asumiremos que llega al destino con un porcentaje de éxito muy alto (100 %), y con retardos típicos de UMTS bajos y sin producir más oberhead en la VANET. Conociendo los rendimientos de UMTS esa aproximación es totalmente justificada.

### Desarrollo de la solución

Se desea desarrollar una extensión para el simulador ns2 cuyo comportamiento sea lo más parecido posible a una plataforma de comunicaciones híbrida con una interfaz IEEE 802.11 con protocolo de encaminamiento AODV y otro interfaz UMTS.

Se ha diseñado un mecanismo para modificar el protocolo AODV y poder contar con un enlace de respaldo por el que cada nodo envíe datos por el enlace prioritario que es el enlace IEEE 802.11 y se utilizará UMTS en caso de que no sea posible llegar al destino a través de la VANET.

El mecanismo consiste en crear una nueva función dentro del protocolo AODV llamada sendUmts. Dicha función recoge el paquete que se iba a tirar (marcado como DROP) y lo envía a una dirección ficticia marcandólo como AODV2. De esta forma, cuando el parse analice la traza generada por el simulador se podrá contabilizar el número de paquetes enviados por este mecanismo.

Es importante notar que no hemos implementado otra interfaz sino que modificando el comportamiento de AODV,se logra que el parse considere que se han mandado por un enlace UMTS.

Los principales cambios afectan a la función de recibir paquetes en la que se añaden unos filtros mediante los cuales:

- Si el propio nodo está generando el paquete y no hay ruta válida para el destino, se manda por UMTS y a la vez se busca una ruta por la VANET enviando un RREQ.
- Si el estado de la ruta hacia un destino es DOWN o ha expirado, se manda por UMTS.

Además de esto, se modifican ciertas funciones del protocolo como *route_link_failed* de forma que cuando se produce un fallo de enlace, en lugar de descartar el paquete se envía por UMTS.

Solo se envían los datos por UMTS desde el origen, es decir si el paquete encuentra un fallo en algún nodo intermedio en la ruta no se manda por UMTS sino que sigue los procedimientos habituales del protocolo original: guardar en el buffer, descartarlo...

Esta solución es ideal para transmisiones UDP ya que los paquetes se envían a una tasa constante y no esperan confirmación del destino, ahora bien presenta problemas en TCP ya que no estamos generando los correspondientes ACK y por lo tanto el rendimiento calculado para la red híbrida será mucho peor que el que tendría en realidad, contando con ACKs de vuelta también por el enlace UMTS. Por lo tanto se prevee resultados de simulaciones muy pesimistas en el caso de transmisiones TCP. Por lo tanto, se observarán únicamente los resultados UDP para concluir si el enlace UMTS introduce mejoras en la red VANET.

# Capítulo 5

# Resultado de las simulaciones

Las simulaciones se han llevado a cabo siguiendo los escenarios descritos en el capítulo 3. Para cada escenario se observa distintos protocolos y sus comportamiento en tres densidades de tráfico (alta, media y baja) con dos protocolos de comunicación (TCP o UDP).

## 5.1. Comunicación entre dos vehículos

En estas simulaciones entran en juego los dos primeros escenarios: comunicaciones VANET pura y comunicaciones VANET a través de nodos intermedios.

En este estudio se simularán diferentes protocolos ad-hoc unicast :

- AODV
- DSDV
- DSR
- FSR
- OLSR

Las características de cada protocolo están descritas en el capítulo 2 del estado del arte, pero es conveniente recordar en este punto a que grupo pertenece cada uno de ellos. AODV y DSR son protocolos reactivos mientras que los demás son proactivos.

Para cada topología se eligen dos nodos dentro de todos los nodos presentes y se creará una conexión entre ellos, primero UDP y luego TCP.

Se ha elegido una aplicación UDP CBR (Constant Bit Rate) ya que se aproxima bien a las aplicaciones UDP que mandan tráfico a una velocidad constante y sin preocuparse de si los paquetes han sido entregados o no. Para simular una conexión TCP se ha elegido una aplicación FTP.

Las características de las conexiones a definir en el fichero tcl son las siguientes:
Para FTP sobre TCP: Se manda paquetes de 1000 bytes. El algoritmo de control de congestión es el TAHOE TCP con una ventana de 20 paquetes.
Para CBR sobre UDP: Se mandan paquetes de 210 bytes a una velocidad de 448 kbps a un interval de 3.75 ms. Se podrá mandar un máximo de 2684353456 paquetes.

Las simulaciones de estas conexiones se realizan con todos los protocolos comparando el rendimiento de cada uno de ellos en términos de porcentajes de entregas (pdfr), retardos extremo a extremo y sobrecarga de las comunicaciones introducido por el protocolo. Se presentarán gráficas tridimensionales de los resultados obtenidos para una aproximación visual del rendimiento de cada protocolo.

Se podrían hacer más comparaciones, por ejemplo, variando la velocidad de los vehículos o introduciendo mayor número de conexiones en la VANET sucesivamente pero consideramos que estos escenarios son suficientemente representativos para nuestro caso de estudio.

Es importante estudiar con detenimiento el escenario antes de llevar a cabo el trabajo. En efecto, hay que asegurarse que los dos nodos que elegimos tienen las mismas posiciones relativas en los distintos escenarios con diferentes flujos de tráfico y diferentes protocolos. Esta condición es imprescindible para que los resultados de la simulación sean viables. Si escogiesemos los nodos al azar el resultado también sería aleatorio: por ejemplo puede ser que los vehículos estén tan lejos que no se vean y no puede llegar ningún paquete o que al revés los nodos estén tan cerca que la conexión sea siempre directa y que el pdfr sea de 100 %.

Se realizan pruebas previas a las simulaciones para determinar los nodos a considerar. Gracias al animador nam podemos observar los esquemas de movilidad. Se observa que los nodos 0 y 1 son los primeros en llegar por cada carril y que al mantener el mismo esquema de velocidades en todos los escanarios, mantienen sus posiciones relativas constantes siendo el número de vehículos entre ellos la única variación.

### 5.1.1. Comunicaciones unicast en circuito urbano

Las conexiones (que sean TCP o UDP) se producen desde el instante 20 hasta el 100 entre el nodo 0 y el nodo 1.

**UDP**

Cuadro 5.1: UDP Unicast en circuito urbano con densidad alta

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 211334 | 19,89 | 0,2787 | 805 |
| AODV | 211334 | 39,14 | 0,5093 | 418 |
| DSR | 211334 | 39,36 | 0,3818 | 1047 |
| OLSR | 211334 | 24,65 | 0,2833 | 4731 |
| FSR | 211334 | 13,44 | 0,0538 | 1170 |

Cuadro 5.2: UDP Unicast en circuito urbano con densidad media

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 211334 | 22,48 | 0,1612 | 1738 |
| AODV | 211334 | 43,84 | 0,3269 | 396 |
| DSR | 211334 | 44,62 | 0,3600 | 124 |
| OLSR | 211334 | 26,97 | 0,3158 | 9103 |
| FSR | 211334 | 12,74 | 0,0786 | 2244 |

Cuadro 5.3: UDP Unicast en circuito urbano con densidad baja

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 211334 | 13,00 | 0,0042 | 1078 |
| AODV | 211334 | 30,41 | 0,2128 | 199 |
| DSR | 211334 | 32,29 | 0,2706 | 223 |
| OLSR | 211334 | 21,33 | 0,1664 | 6132 |
| FSR | 211334 | 12,89 | 0,0295 | 1716 |

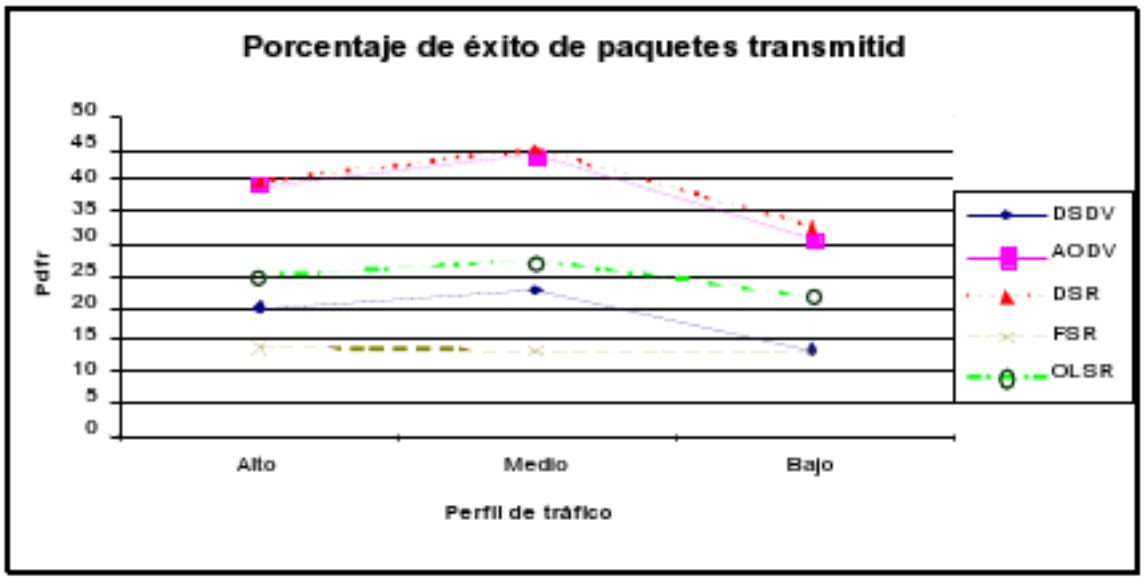



Figura 5.1: Porcentaje de éxito unicast UDP en circuito urbano

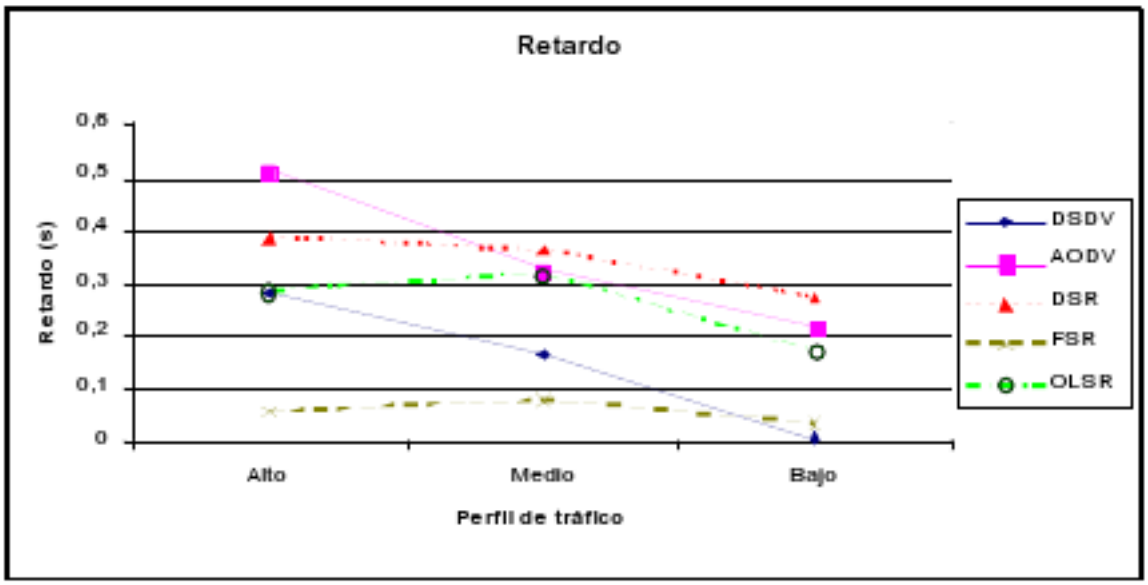



Figura 5.2: Retardo unicast UDP en circuito urbano

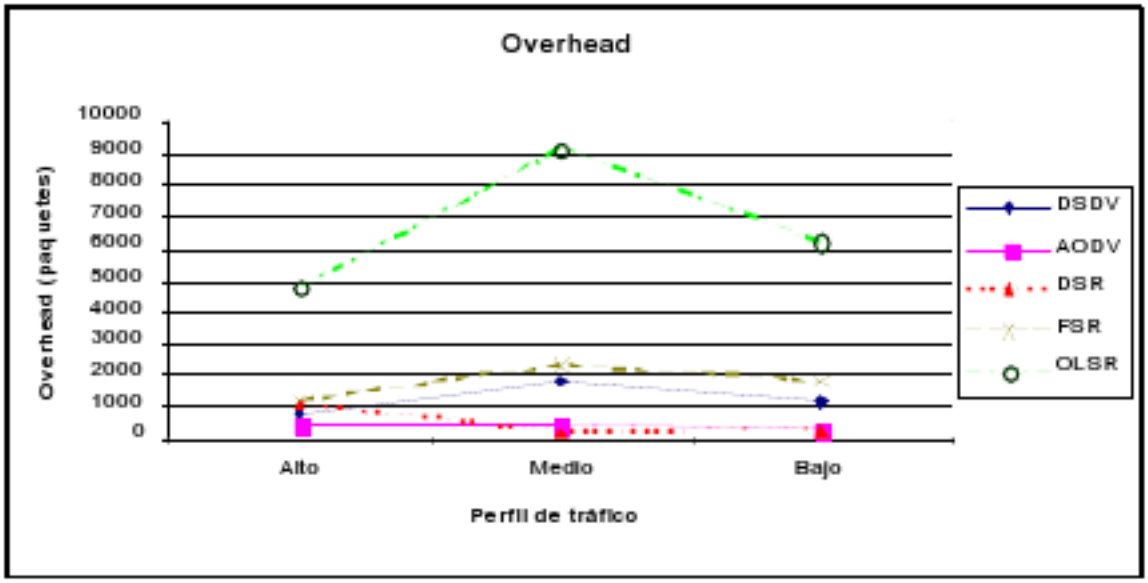



Figura 5.3: Overhead unicast UDP en circuito urbano

Se puede observar que para el escenario considerado, se obtiene un óptimo comportamiento en el perfil medio. Vemos, en efecto, que es dentro de este escenario que el porcentaje de entrega es mayor para todos los protocolos. También se observa que los protocolos reactivos presentan mayor porcentaje de éxito, menores retardo y overhead. Estos resultados coinciden con lo previsto ya que en las VANET, donde los cambios de topologías son muy frecuentes, los protocolos proactivos se quedan rápidamente obsoletos. Veamos más en detalle las conclusiones de cada gráfica:

- Porcentaje de éxito: Se nota una diferencia muy clara entre los protocolos reactivos (DSR seguido muy de cerca por AODV) y los protocolos proactivos. Los protocolos reactivos presentan mejores tasas de entregas de paquetes. Podemos notar que para el protocolo FSR las tasas de entregas son casi constantes, no aumentan a aumentar la densidad de coches. Eso significa que FSR no reacciona bien ante los cambios de topología y no es capaz de optimizar las rutas con los nuevos nodos que aparecen entre el emisor y el receptor. Por otro lado, en situaciones de poco tráfico el pdfr disminuye. Eso es así porque al haber menos nodos entre emisor y receptor no hay comunicación cuando los nodos se encuentran a una distancia demasiada grande.

- Comparativa de los retardos: La primera constatación que se puede hacer es que con perfiles de tráfico bajos, los retardos disminuyen de forma significativa para todos los protocolos. Si es cierto que menos paquetes llegan al destino, los que lo hacen presentan menos retardos ya que pasan por menos nodos intermedios antes de alcanzar el destino. Los protocolos reactivos, aunque presentan pdfr mejores, introducen retardos mayores. Eso se explica por el hecho de que consiguen rutas actualizadas y más frescas pero que el mecanismo de descubrimiento de rutas que se lleva a cabo cada vez que se tiene que mandar un paquete introduce retardos de transmisiones. Dentro de los protocolos reactivos, AODV tiene retardos menores que DSR salvo en el perfil de tráfico alto.

- Overhead: En la gráfica de sobrecarga, llama la atención el comportamiento de OLSR que presenta un overhead muy por encima de los demás protocolos. Por lo tanto podemos concluir que su uso no es recomendable es esos entornos. Los protocolos reactivos cargan menos la red.

### TCP

En el caso de las conexiones TCP, aparece el throughput que mide el número de paquete que ha sido capaz de enviar el nodo origen. Este indicador es quizás el más importante ya que indica que el protocolo ha sido capaz de

enviar mayor cantidad de información y el resto de los indicadores deberán ser estudiados teniendo muy en cuenta este dato.

Cuadro 5.4: TCP Unicast en circuito urbano con densidad alta

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 903 | 98,11 | 0,1395 | 796 |
| AODV | 2704 | 97,56 | 0,21051 | 1239 |
| DSR | 912 | 98,79 | 0,1220 | 41 |
| OLSR | 1713 | 96,15 | 0,1801 | 4666 |
| FSR | 860 | 98,95 | 0,1196 | 1170 |

Cuadro 5.5: TCP Unicast en circuito urbano con densidad media

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 863 | 97,91 | 0,1308 | 1785 |
| AODV | 2824 | 97,38 | 0,2381 | 570 |
| DSR | 2181 | 98,71 | 0,2818 | 299 |
| OLSR | 1547 | 93,73 | 0,1371 | 9353 |
| FSR | 850 | 96,71 | 0,0832 | 2244 |

Cuadro 5.6: TCP Unicast en circuito urbano con densidad baja

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 856 | 98,83 | 0,1885 | 1117 |
| AODV | 1865 | 98,18 | 0,1753 | 398 |
| DSR | 1262 | 99,84 | 0,2305 | 630 |
| OLSR | 1301 | 96,77 | 0,1519 | 6084 |
| FSR | 847 | 98,35 | 0,0961 | 1716 |

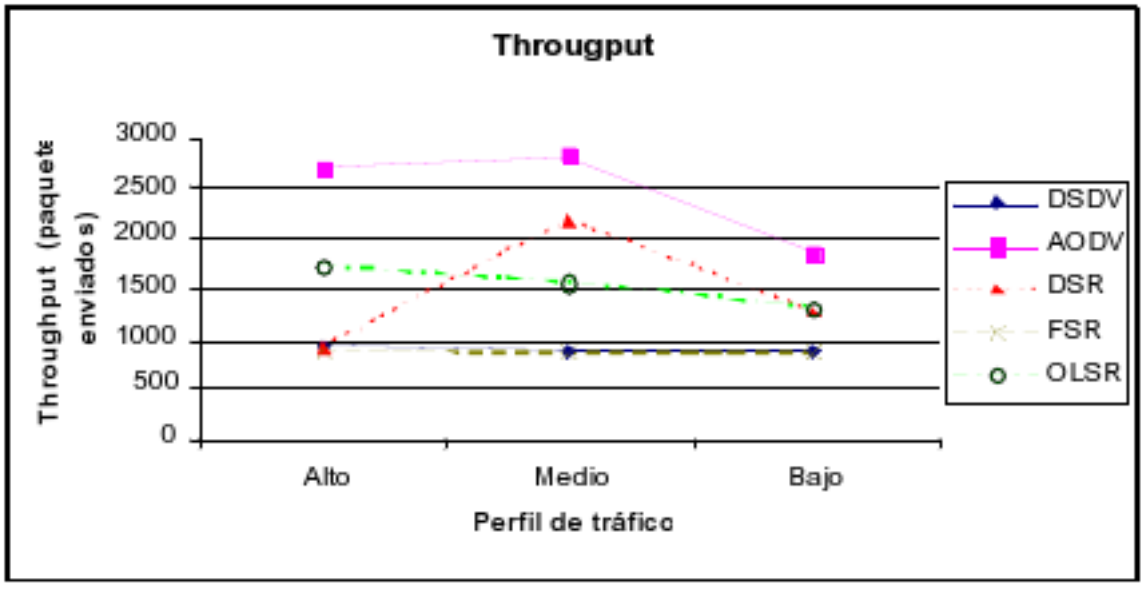



Figura 5.4: Througput unicast TCP en circuito urbano

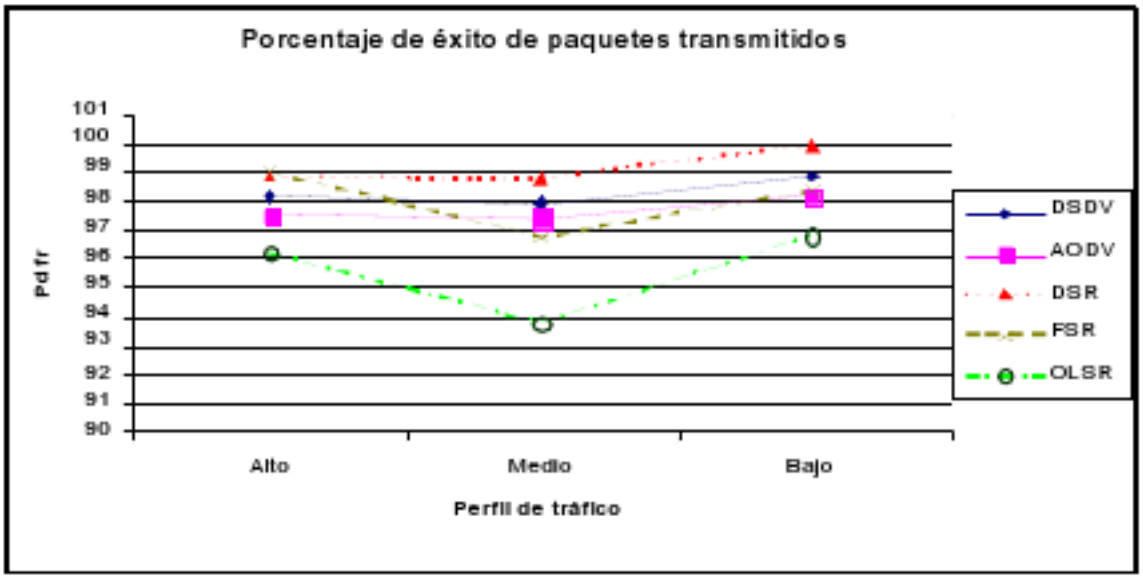



Figura 5.5: Porcentaje de éxito unicast TCP en circuito urbano

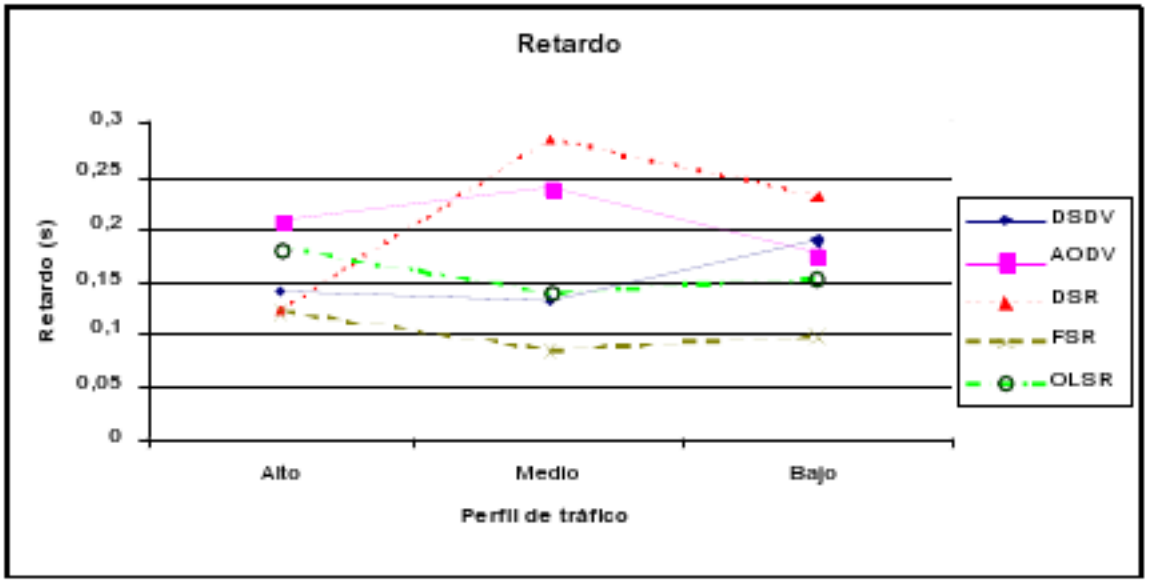



Figura 5.6: Retardo unicast TCP en circuito urbano

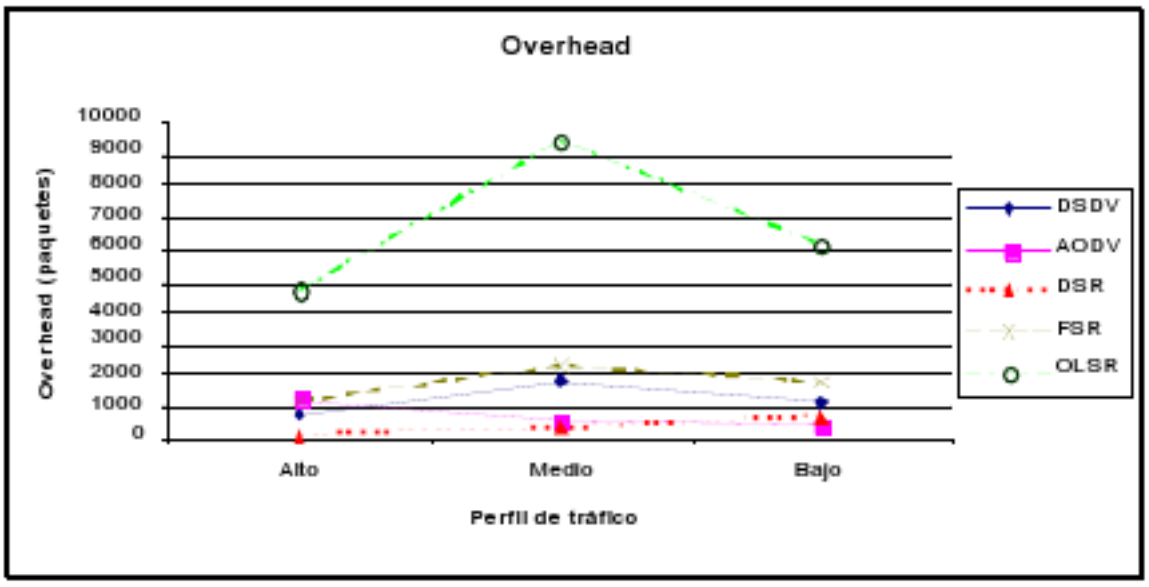



Figura 5.7: Overhead unicast TCP en circuito urbano

Se observa que para el circuito definido aparece un máximo local de rendimiento con el perfil de tráfico medio, con el que mayor densidad de información se consigue mandar. Una vez más y de forma general, los protocolos reactivos presentan mejores prestaciones, con la excepción de FSR con densidad alta de nodos que presenta un comportamiento parecido al de los reactivos. Detallamos cada gráfica:

- Throughput: El claro vencedor es AODV que consigue mandar más información que DSR, sobre todo con densidades altas y por supuesto que los protocolos proactivos. Volvemos a llegar a la misma conclusión que en UDP: los protocolos proactivos reaccionan mal frente a cambios de topología de la VANET ya que no son capaces de actualizar las rutas lo suficientemente rápido.

- Pdfr: El mejor protocolo en este caso es DSR, seguido de DSDV, AODV, FSR y OLSR respectivamente. Eso significa que aunque AODV consigua mantener su throughput, su porcentaje de éxito es menor, pierde más paquetes que el protocolo proactivo DSDV. OLSR vuelve a presentar prestaciones muy inferiores al resto de los protocolos.

- Retardos: Los protocolos que consiguen mandar mayor cantidad de información presentan retardos mayores, salvo en el caso de AODV cuyos retardos extremo a extremo son menores que los de DSR. Fijándose en AODV se observan valores entre 0,2 y 0,25 segundos de media, un retardo acceptable dada la cantidad de información que se manda a través de la VANET.

- Overhead: OLSR vuelve a destacar por su excesiva sobrecarga. Los protocolos reactivos siguen presentando overhead memores, en particular en el caso de DSR.

### 5.1.2. Comunicaciones unicast en autopista

En este estudio se pretende comparar los protocolos ad-hoc con diferentes perfiles de tráfico en la autopista, para ello se establecen dos comparativas, una conexión FTP sobre TCP y otra CBR sobre UDP modificando las densidades de tráfico para ambos caso.

Ambas conexiones (tanto TCP como UDP) se producen entre el instante 10 hasta el 90 entre el nodo 0 y el nodo 2.

**UDP**

Cuadro 5.7: UDP Unicast en autopista con densidad alta

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 21334 | 24,16 | 0,0251 | 2876 |
| AODV | 21334 | 32,83 | 0,1183 | 1751 |
| DSR | 21334 | 29,02 | 0,1064 | 2281 |
| OLSR | 21334 | 22,77 | 0,1995 | 10318 |
| FSR | 21334 | 22,07 | 0,1130 | 2604 |

Cuadro 5.8: UDP Unicast en autopista con densidad media

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 21334 | 18,46 | 0,1166 | 3309 |
| AODV | 21334 | 25,27 | 0,1700 | 3324 |
| DSR | 21334 | 28,38 | 0,4753 | 5794 |
| OLSR | 21334 | 16,03 | 0,2277 | 10926 |
| FSR | 21334 | 15,32 | 0,1243 | 2604 |

Cuadro 5.9: UDP Unicast en autopista con densidad baja

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 21334 | 23,91 | 0,0692 | 2096 |
| AODV | 21334 | 48,12 | 0,3033 | 1438 |
| DSR | 21334 | 44,98 | 0,3772 | 3712 |
| OLSR | 21334 | 31,75 | 0,2277 | 9054 |
| FSR | 21334 | 21,50 | 0,0957 | 1860 |

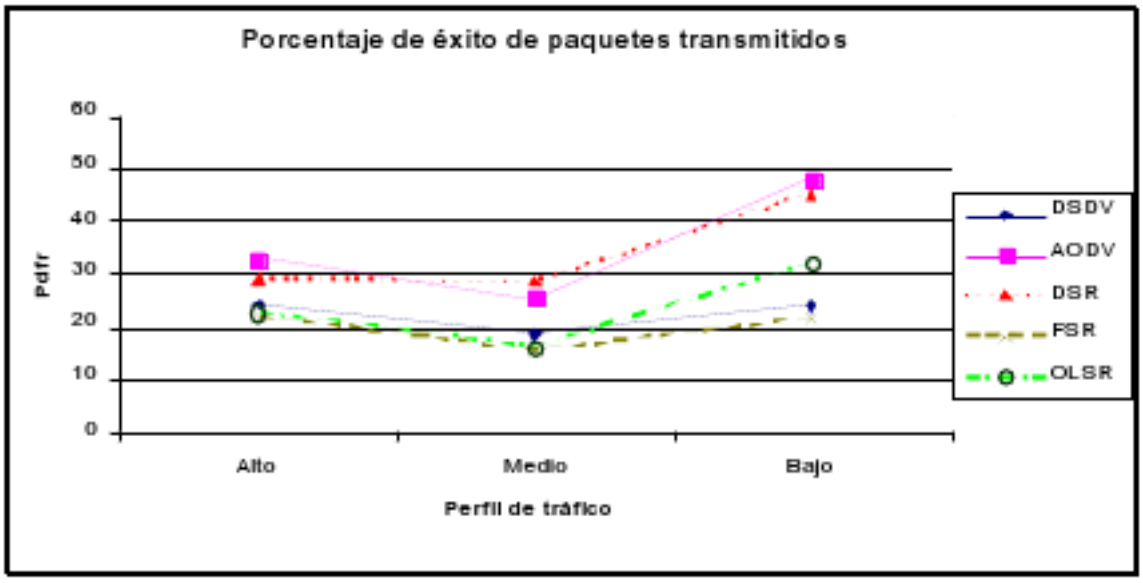



Figura 5.8: Porcentaje de éxito unicast UDP en autopista

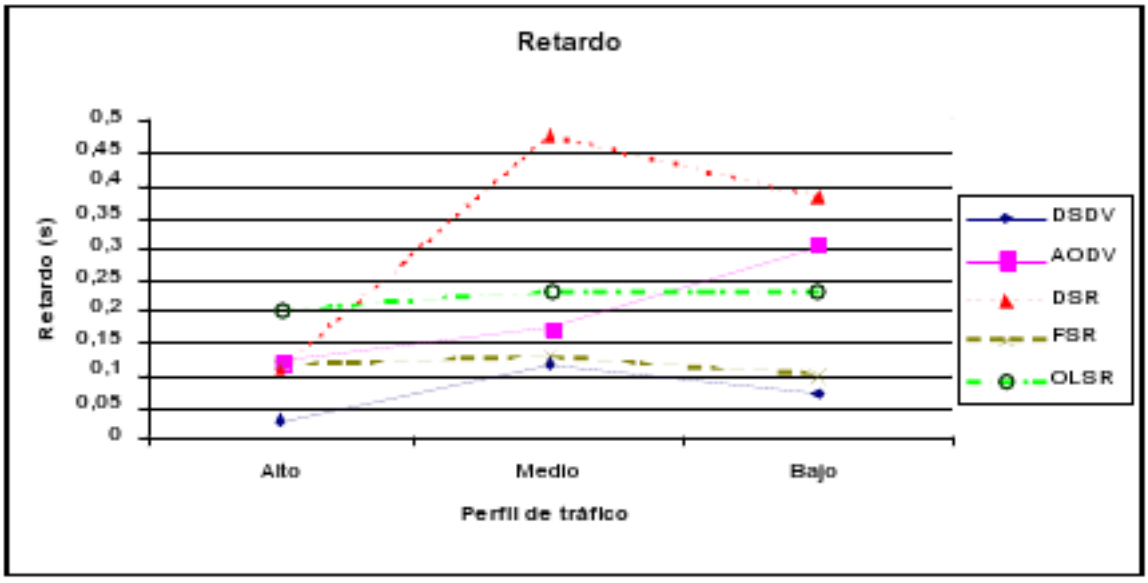



Figura 5.9: Retardo unicast UDP en autopista

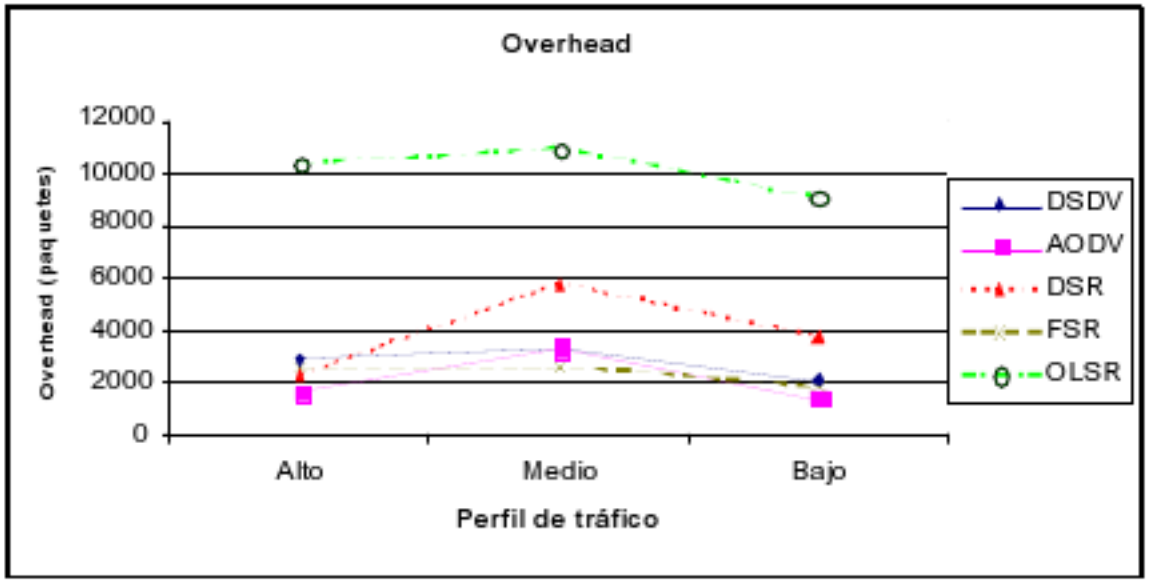



Figura 5.10: Overhead unicast UDP en autopista

Observando las gráficas se concluye que para la autopista y los perfiles de tráfico UDP definidos, se obtienen buenos comportamientos con densidad de tráfico baja, dónde el porcentaje de éxito se acerca al 50 % en el caso de AODV. Este protocolo, de forma clara, se presenta como claro vencedor en el estudio de UDP, seguido del otro protocolo reactivo DSR. Veamos en detalle las conclusiones de cada gráfica:

- Pdfr: El mejor comportamiento lo tiene AODV, seguido de DSR, DSDV, OLSR y FSR.
- Retardos: AODV presenta retardos acceptables entre 0,1 y 0,3 inferiores incluso a los de algún protocolo proactivo como OLSR con mucho menor porcentaje de éxito. También se ve a simple vista unos valores bastante elevados de retardo de DSR, sobre todo para densidades de tráfico medias. Esto puede ser debido a que este protocolo consiga enviar tráfico utilizando una ruta con elevado número de saltos, aumentando la media de este indicador considerablemente.
- Overhead: el protocolo con mejor comportamiento es AODV, seguido de FSR, DSDV y DSR. Una vez más OLSR genera una sobrecarga en la red desproporcionada para los rendimiemtos que proporciona. Al igual que pasaba en el circuito urbano los protocolos proactivos mantienen un overhead casi constante al variar la densidad de nodos mientras que los reactivos son más sensibles a esta variación.

**TCP**

Cuadro 5.10: TCP Unicast en autopista con densidad alta

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 1562 | 99,36 | 0,1339 | 2879 |
| AODV | 1962 | 98,27 | 0,1184 | 1009 |
| DSR | 1805 | 98,67 | 0,1596 | 63 |
| OLSR | 1407 | 98,58 | 0,2040 | 10293 |
| FSR | 1396 | 98,88 | 0,1238 | 2604 |

Cuadro 5.11: TCP Unicast en autopista con densidad media

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 1131 | 98,59 | 0,1168 | 3039 |
| AODV | 1687 | 96,92 | 0,1802 | 2195 |
| DSR | 1338 | 99,78 | 0,1746 | 87 |
| OLSR | 971 | 99,18 | 0,1277 | 11301 |
| FSR | 993 | 97,28 | 0,1541 | 2604 |

Cuadro 5.12: TCP Unicast en autopista con densidad baja

| ***Protocolo*** | ***Paq. enviados*** | ***Pdfr( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** |
|---|---|---|---|---|
| DSDV | 5274 | 99,77 | 0,1400 | 2200 |
| AODV | 5742 | 99,96 | 0,1347 | 87 |
| DSR | 5399 | 99,02 | 0,1348 | 43 |
| OLSR | 4763 | 99,56 | 0,1532 | 8856 |
| FSR | 4819 | 99,46 | 0,1194 | 1860 |

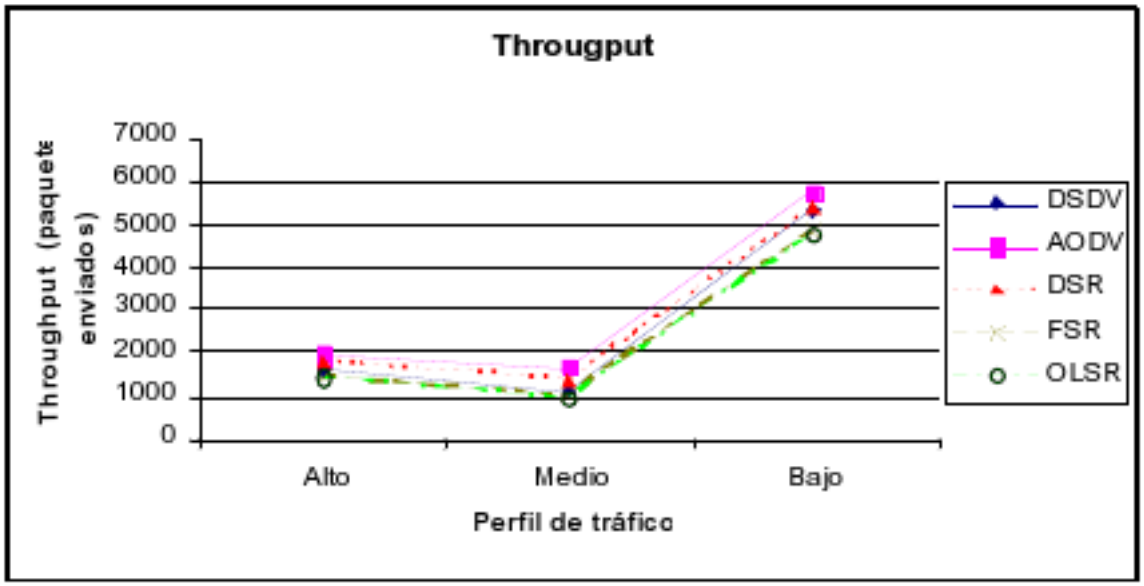



Figura 5.11: Througput unicast en autopista

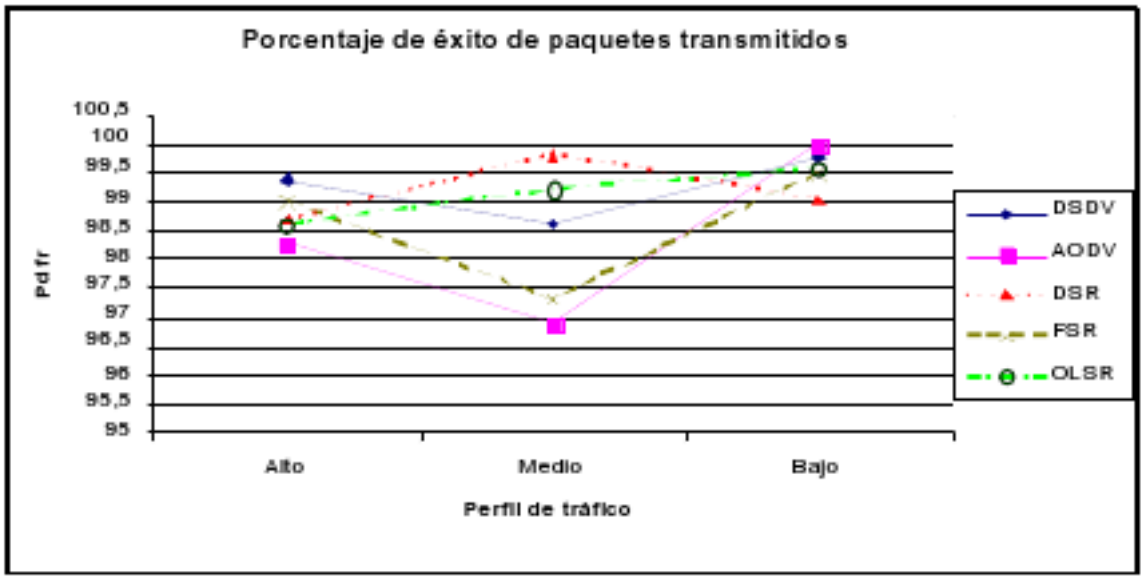



Figura 5.12: Porcentaje de éxito unicast TCP en autopista

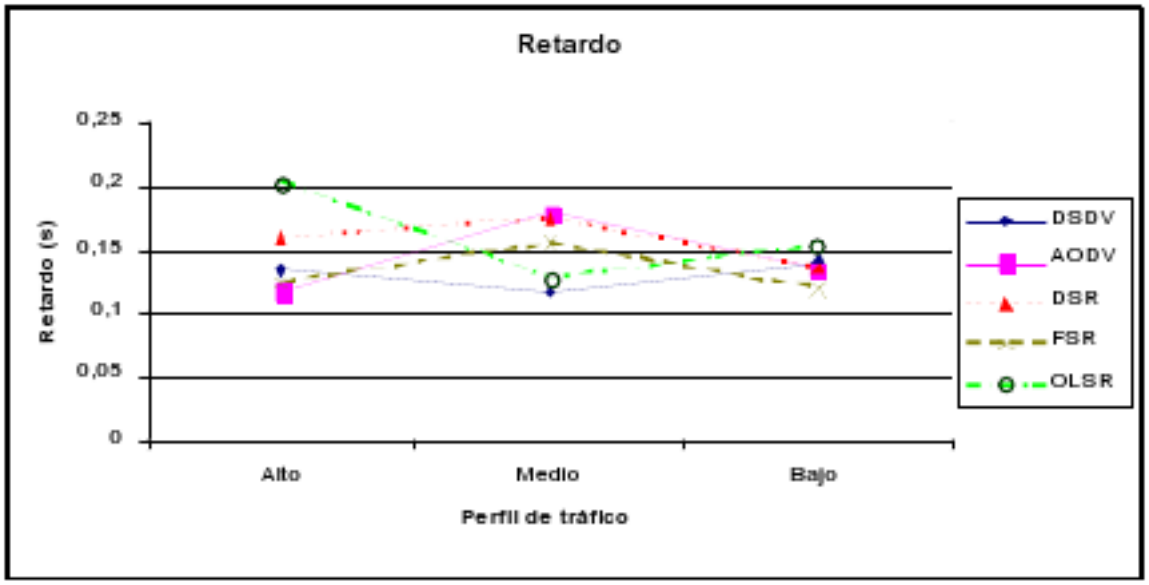



Figura 5.13: Retardo unicast TCP en autopista

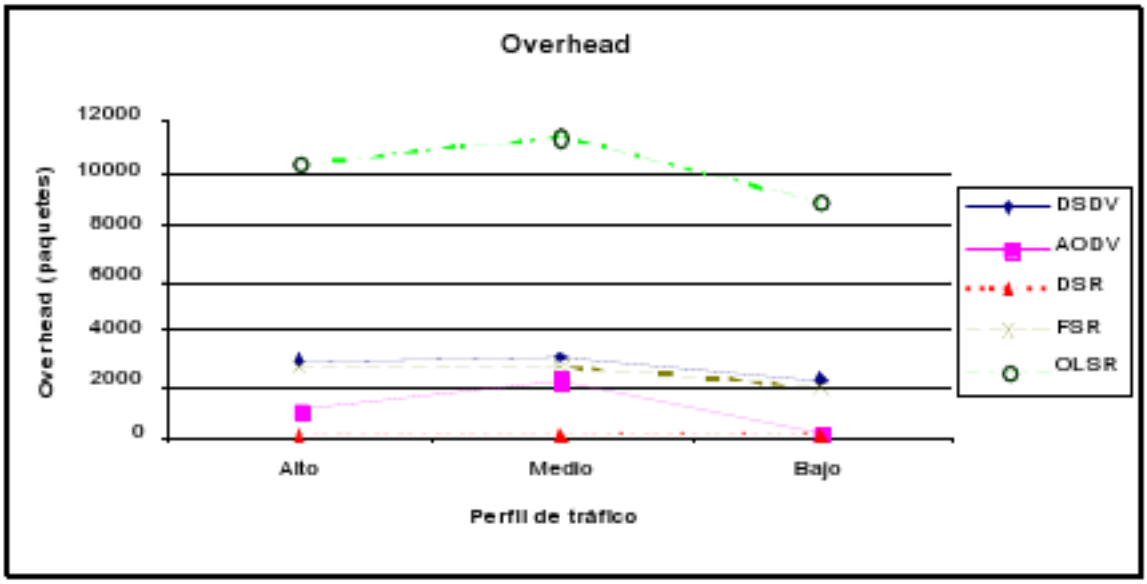



Figura 5.14: Overhead unicast TCP en autopista

Se observa que los mejores valores de transferencia de datos TCP en autopista se dan con el perfil de tráfico bajo dónde todos los protocolos aumentan considerablemente su rendimiento. Una vez más, AODV seguido de FSR dan los mejores resultados en este estudio. Veamos más en detalle las conclusiones de cada gráfica:

- Throughput: Todos los protocolos siguen la misma línea general con una diferencia no muy grande entre todos ellos, esto significa que la mayor parte de los datos transmitidos lo han hecho en circunstancias en las que todos los protocolos funcionan igual, probablemente con el mismo número de nodos intermedios.

- Pdfr: Se vuelve a apreciar que AODV tiene un mal porcentaje en comparación con el resto para densidades altas y medias. En cambio DSR y OLSR presentan buenos porcentajes.

- Retardo: Los protocolos reactivos tienen un máximo para el prefil de tráfico medio, esto significa que consiguen enviar información por una ruta que tarda más tiempo en llegar al destino, pero lo alcanza, aumentando en promedio este indicador.

- Overhead: Vuelve a aparecer la excesiva carga de la red por parte de OLSR, manteniéndose baja la carga de ambos protocolos reactivos. FSR presenta una sobrecarga realmente baja.

### 5.1.3. Conclusiones generales de la comparativa de protocolos unicast

La principal conclusión de es este estudio es que en esos entornos de topología muy variable, los protocolos reactivos AODV y DSR presentan prestaciones mayores que los protocolos proactivos. Resulta más eficiente llevar a cabo un mecanismo de descubrimiento de rutas sobre demanda que intentar tener tablas actualizadas de ruta en cada momento. En efecto, con un protocolo proactivo, si los cambios de topología son rápidos, se multiplican los mensajes de control introduciendo una sobrecarga excesiva, se pueden perder más paquetes.

Dentro de los protocolos reactivos, AODV presenta, en la mayoría de las topologías, las mejores tasas de transferencia; bajos retardos y no genera grandes cantidades de paquetes de control para la creación y el mantenimeinto de las rutas, se concluye que es el más eficiente para estas comunicaciones en general.

En todos los estudios se observa que el perfil de tráfico óptimo es el perfil medio. Si aumenta la densidad de tráfico la VANET se satura y si disminuye el número de nodos se reducen las rutas para llegar al destino en ciertos instantes de tiempo lo que supone pérdidas de paquetes o aumento de los retardos de transmisión.

Tanto en UDP como en TCP, los protocolos reactivos logran mandar mayor cantidad de datos. AODV alcanza en UDP un porcentaje de éxito de 50 % en el mejor de los casos (densidad baja en autopistas) y un throughput de 6000 paquetes en TCP. Estos valores se observan durante los 80 segundos que dura la simulación, por lo tanto equivalen a tasas medias de 30kbps para UDP y 70kbps para TCP.

Se ha comprobado que en muchas ocasiones, los retardos son inversamente proporcionales a la cantidad de información transmitida ya que para conseguir que el paquete llegue a su destino los protocolos se ven muchas veces obligados a mandar el tráfico por rutas más largas, aumentando así la media de los retardos de transmisiones. Aún así, los retardos que presenta AODV, excepto en el circuito urbano con conexión UDP y perfil de tráfico alto, se mantienen entre 100 y 200 ms para todas las topologías.

En cuanto a overhead, los protocolos proactivos presentan una mayor carga a la red siendo casi constante al modificar los perfiles de tráfico mientras que los reactivos introducen menos carga y son más sensibles a la densidad de nodos. Esta sensibilidad hace que el porcentaje de paquetes de control vaya del 2 % en el mejor de los casos hasta al 30 % en el peor de los casos. DSR destaca por su buen comportamiento en comunicaciones TCP.

## 5.2. Comunicación entre un vehículo y la infraestructura vial. Difusión de mensajes.

En este estudio nos centramos en la comparativa de los protocolos geocast en los dos tipos de vías anteriormente descritas: circuito y autopista. La finalidad de los protocolos geocast es enviar información desde un nodo a todos aquellos que se encuentren en una determinada área geográfica conocida como zona de geocast. Para conseguirlo es necesario que todos los nodos conozcan su localización en todo momento, utilizando por ejemplo el GPS (Global Positioning System) o el futuro Galileo.

Simulamos los siguientes protocolos:

- LBM-Box
- LBM-step
- GAMER
- GEOGRID

En todos los escenarios de simulación de este capítulo se ha utilizado un rango de transmisión de 250 metros y el ancho de banda de enlace de cada nodo es de 2Mbps. Fijamos un nodo estático origen de los datos que manda paquetes CBR geocast de 64 bytes.

Los indicadores que hemos considerado para este estudio son los siguientes:

- One Success Rate (OSDR): Si el nodo origen envía datos y al menos uno de los nodos de la zona geocast los recibe se produce un éxito. Este indicador se aproxima a los resultados para All Success (cuando todos los nodos de la zona geozast reciben el paquete) ya que son muy similares.
- Overhead: suma de todos los paquetes transmitidos (datos y control) por todos los nodos en la simulación y divididos por los éxitos.
- Retardo por éxito.
- Número de saltos.

### 5.2.1. Protocolos geocast en circuito urbano

En este estudio se pretende comparar los protocolos de tráfico en el circuito urbano, para ello se fija la tasa de envío de paquetes desde el nodo origen a un valor intermedio; 40 paquetes por segundos y se modifican únicamente las densidades de tráfico. Definimos los mismos modelos de movilidad que para el estudio unicast salvo que fijamos dos nodos estáticos: un nodo origen de datos, el gateway en la posición (450,0) y un nodo fijo dentro de la zona geocast (919, 519) para asegurarnos de que siempre exista un nodo en dicha zona. Definimos la zona de geocast se define como un rectángulo delimitado por las coordenadas (820,470) y (920, 520). Se usa el protocolo UDP para todos los escenarios ya que es el protocolo usado en situaciones reales de geocasting, el protocolo TCP generando demasiado overhead.

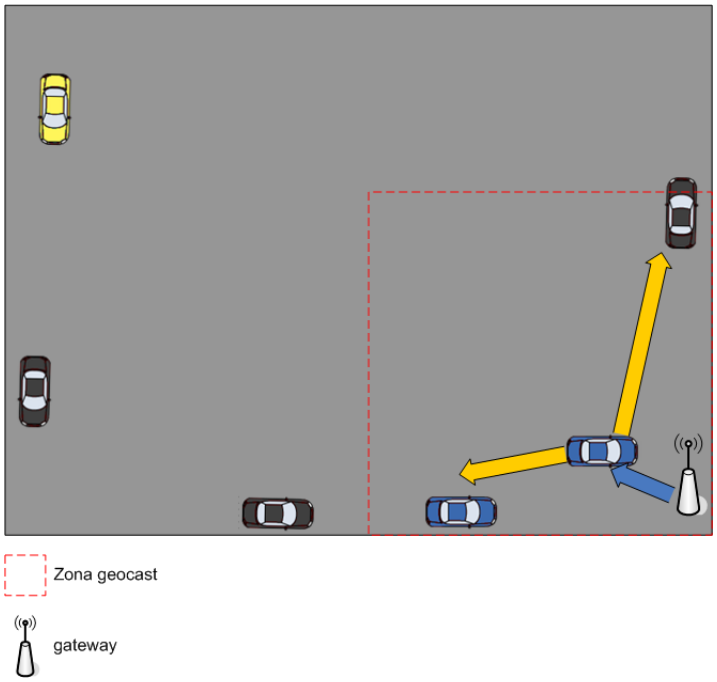



Figura 5.15: Esquema geocast en circuito urbano

Cuadro 5.13: Geocast en circuito urbano con densidad alta

| ***Protocolo*** | ***Paq. enviados*** | ***OSDR( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** | ***Hops*** |
|---|---|---|---|---|---|
| LBM-Box | 4800 | 98,27 | 0,0122 | 9 | 5,34 |
| LBM-Step | 4800 | 94,91 | 0,0144 | 12 | 5,32 |
| GAMER | 4800 | 91,47 | 0,0127 | 11 | 5,22 |
| GEOGRID | 4800 | 76,12 | 0,0129 | 16 | 6,07 |

Cuadro 5.14: Geocast en circuito urbano con densidad media

| ***Protocolo*** | ***Paq. enviados*** | ***OSDR( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** | ***Hops*** |
|---|---|---|---|---|---|
| LBM-Box | 4800 | 88,79 | 0,0108 | 8 | 4,81 |
| LBM-Step | 4800 | 81,89 | 0,0193 | 15 | 4,89 |
| GAMER | 4800 | 84,72 | 0,0144 | 12 | 5,03 |
| GEOGRID | 4800 | 62,45 | 0,0136 | 17 | 6,07 |

Cuadro 5.15: Geocast en circuito urbano con densidad baja

| ***Protocolo*** | ***Paq. enviados*** | ***OSDR( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** | ***Hops*** |
|---|---|---|---|---|---|
| LBM-Box | 4800 | 16,08 | 0,0025 | 14 | 1,26 |
| LBM-Step | 4800 | 56,75 | 0,0221 | 19 | 5,72 |
| GAMER | 4800 | 58,62 | 0,0151 | 13 | 5,50 |
| GEOGRID | 4800 | 31,95 | 0,0159 | 23 | 7,28 |

Aunque hemos recogido datos de retardos y de número de saltos, estos datos no se reflejan en la comparativa gráfica ya que consideramos que son medidas de promedio y que no son muy significativos de las prestaciones reales de los protocolos.

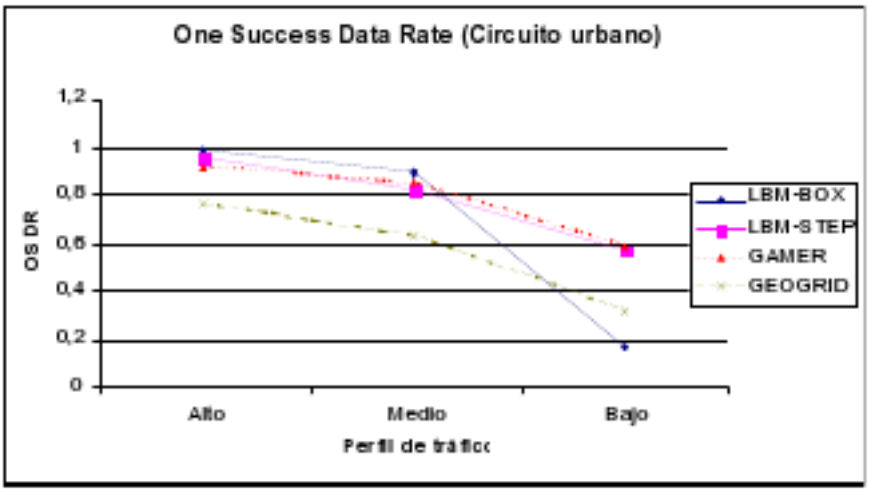



Figura 5.16: OSDR en protocolos geocast en circuito

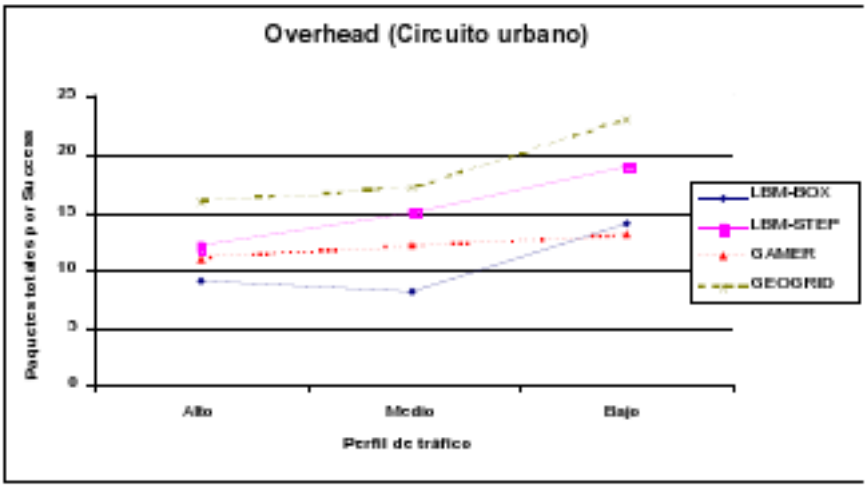



Figura 5.17: Overhead en protocolos geocast en circuito

Observando las gráficas, se nota claramente que las prestaciones de todos los protocolos considerados bajan de forma significativa con la densidad de tráfico. Bajan los porcentajes de éxito a la entrega y aumentan los overhead. Para todos los protocolos, el perfil de tráfico óptimo es el perfil alto. Se explica por el hecho de que cuando muchos vehículos se encuentran en la zona geocast, el broadcasting es más eficiente ya que se disponen de más

rutas hacia un mismo destino, los porcentajes de éxito se aproximan entonces al 100 %.

Examinando las gráfica de los OSDR, se puede decir que en perfil de tráfico alto, el protocolo que mejores prestaciones ofrece es LBM-Box, seguido de cerca por LBM-step y GAMER, GEOGRID presenta prestaciones peores. Cuando la densidad de tráfico es baja, se hunden las prestaciones de LBM-Box. Esto se explica probablemente por la manera de considerar la zona de forwarding que tiene LBM-Box. LBM-Box construye la zona de forwarding considerando el rectángulo mínimo que contiene el nodo origen y la zona geocast. Cuando hay pocos vehículos en el escenario, se reduce el número de vehículos en la zona de forwarding y el paquete no consigue llegar a la zona geocast. LBM-step o GAMER son soluciones más robustas en perfiles de tráfico bajos. En la siguiente figura se observa como la zona de forwarding de A se vacía cuando la densidad de los nodos es menor.

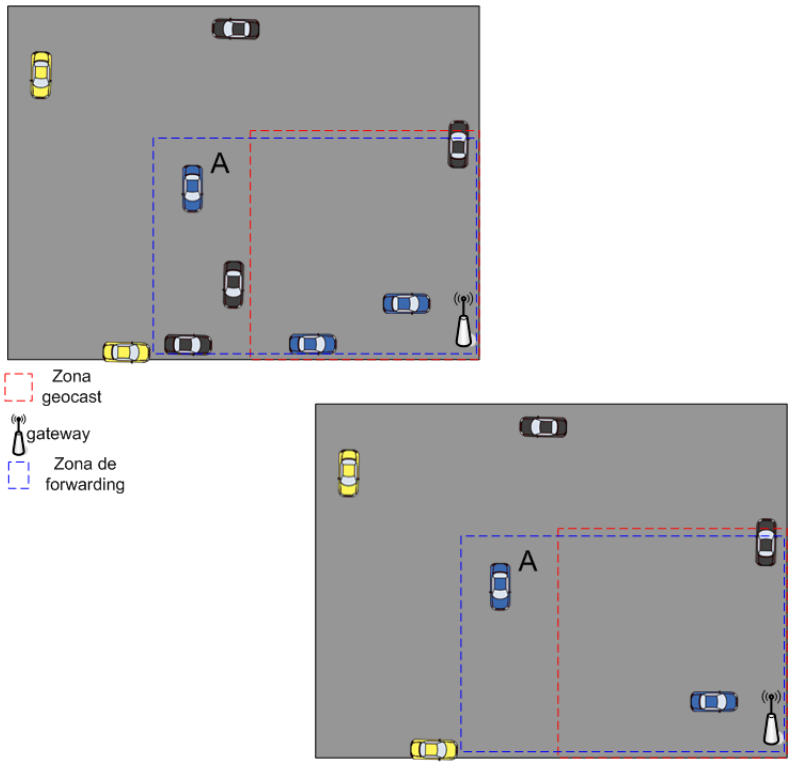



Figura 5.18: Bajada de prestaciones de LBM-Box con densidades de tráfico bajas

De manera general la sobrecarga introducida en la red aumenta para los perfiles de tráfico más bajos. Si la densidad de nodos disminuye, existen menos rutas y el proceso de descubrimiento y de mantenimiento es más costoso.

Los que menor overhead presentan son LBM-box, Gamer LBM-step y Geogrid; con la excepción del escenario con tráfico bajo dónde al disminuir el porcentaje de éxitos el overhead realtivo de LBM-Box aumenta por encima del de Gamer.

### 5.2.2. Protocolos geocast en autopista

En este estudio, queremos comparar los protocolos de diferentes perfiles de tráfico en autopistas, para ello se considera el mismo esquema de movilidad que en el estudio de protocolos unicast a la diferencia que se fija un nodo estático (gateway) en la posición (1000, 0). El gateway transmite 40 paquetes UDP por segundos. Se fija otro nodo estático en la zona geocast (2000, 1) para asegurarse de que siempre exista un nodo en dicha zona. La zona geocast para este estudio es el rectángulo definido por los siguientes puntos (1750, 0) y (2250, 30).

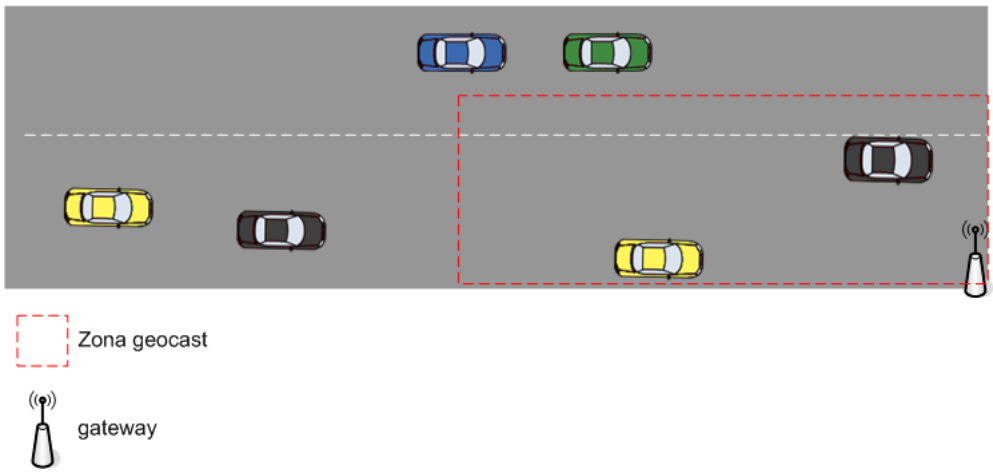



Figura 5.19: Esquema geocast en autopista

Cuadro 5.16: Geocast en autopista con densidad alta

| ***Protocolo*** | ***Paq. enviados*** | ***OSDR( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** | ***Hops*** |
|---|---|---|---|---|---|
| LBM-Box | 4800 | 70,52 | 0,0125 | 22 | 1,95 |
| LBM-Step | 4800 | 70,64 | 0,0135 | 22 | 1,92 |
| GAMER | 4800 | 66,40 | 0,0085 | 20 | 1,80 |
| GEOGRID | 4800 | 88,67 | 0,0048 | 12 | 1,94 |

Cuadro 5.17: Geocast en autopista con densidad media

| ***Protocolo*** | ***Paq. enviados*** | ***OSDR( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** | ***Hops*** |
|---|---|---|---|---|---|
| LBM-Box | 4800 | 80,18 | 0,0275 | 21 | 2,28 |
| LBM-Step | 4800 | 79,96 | 0,030 | 21 | 2,30 |
| GAMER | 4800 | 76,31 | 0,0086 | 19 | 2,14 |
| GEOGRID | 4800 | 91,77 | 0,0049 | 12 | 2,15 |

Cuadro 5.18: Geocast en autopista con densidad baja

| ***Protocolo*** | ***Paq. enviados*** | ***OSDR( %)*** | ***Retardo(s)*** | ***Overhead(paquetes)*** | ***Hops*** |
|---|---|---|---|---|---|
| LBM-Box | 4800 | 95,16 | 0,0073 | 14 | 2,07 |
| LBM-Step | 4800 | 94,89 | 0,073 | 14 | 2,05 |
| GAMER | 4800 | 95,15 | 0,0045 | 12 | 1,88 |
| GEOGRID | 4800 | 98,91 | 0,0040 | 10 | 2,08 |

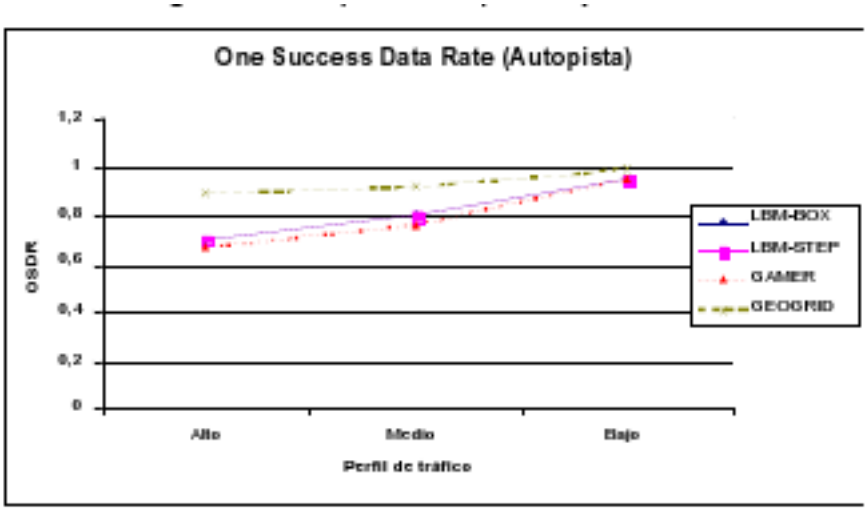



Figura 5.20: OSDR en protocolos geocast en autopista

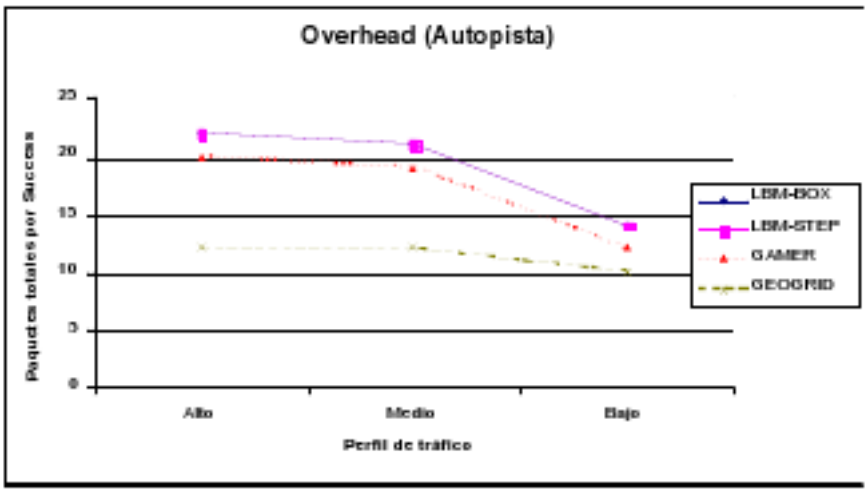



Figura 5.21: Overhead en protocolos geocast en autopista

De todas las gráficas se concluye que el perfil de tráfico óptimo para la autopista es claramente el perfil de tráfico bajo. Se observa que al disminuir el tráfico el porcentage de éxito se aproxima a los 100 % reduciendo significativamente el overhead relativo. Es interesante destacar que los dos esquemas de LBM se comportan de manera casi similar, es decir la alta movilidad les afecta de la misma manera; perdiendo sus buenas prestaciones en comparación con Geogrid.

Considerando los OSDR de los protocolos, por primera vez Geogrid se perfila como claro ganador. El mecanismo de dividir el área de simulación en celdas y elegir un gateway por cada una de ellas hace que este protocolo se

muestre más robusto en condiciones de alta movilidad y de velocidades elevadas. Tras él se encuentran los dos esquemas de LBM y Gamer, las variaciones rápidas de la topología les afectan más que al resto.

De la gráfica de overhead vuelve a salir Geogrid como claro favorito, es el menos sensible a la alta movilidad de este escenario. Posteriormente están Gamer y LBM respectivamente.

### 5.2.3. Conclusiones generales de la comparativa de protocolos geocast

Del estudio que se ha llevado a cabo se concluye que para cada escenario existe una situación de perfil de tráfico óptima: densidad alta para el circuito urbano y densidad baja para la autopista.

Una vez más comprobamos que el rendimiento de un protocolo, es decir su porcentaje de éxito en entregas y el overhead están relacionados. Cuando más pérdida de paquetes se producen, el protocolo se ve obligado a aumentar los paquetes de control para reparar o encontrar nuevas rutas.

En escenarios de circuito urbano el claro ganador es LBM. Gracias a su mecanismo adaptativo de definición de zona de forwarding, logra ser un protocolo robusto y flexible en tales escenarios.

Sin embargo, en casos de autopista destaca el protocolo Geogrid. Gracias a su mecanismo de partición del área se muestra mucho más robusto a las severas condiciones de movilidad relativas a este entorno.

## 5.3. Comunicaciones VANET con respaldo UMTS

En este esudio queremos comparar si introduciendo un enlace de respaldo UMTS a las comunicaciones VANETs se mejoran las prestaciones de la red. Vamos a estudiar el comportamiento de un protocolo AODV modificado desarrollado por Telefónica I+D. AODV modificado funciona de la siguiente manera: envía el tráfico por el enlace Wifi cada vez que sea posible,si se detecta que el tiempo respuesta de una ruta es mayor a un prefijo, se envía la información a través de un enlace de respaldo UMTS. Se ha elegido un mecanismo de encaminamiento AODV por sus buenas prestaciones en las comunicaciones unicast.

### 5.3.1. Comunicaciones en circuito urbano

En este estudio se pretende simular comunicaciones usando el protocolo AODV modificado para ofrecer respaldo UMTS. Compararemos los resul-

tados obtenidos con los del estudio de VANET pura con AODV original. Esperemos demostrar que introduciendo un enlace de respaldo UMTS logramos mejorar el rendimiento de la VANET. Para poder llevar la comparativa de manera rigurosa, simularemos los mismos escenarios que en el caso de los protocolos unicast.

Solo se envían datos UMTS desde el origen, es decir si se encuentra un fallo en un algún nodo intermedio de la ruta se seguirán los procedimientos habituales del protocolo original AODV: guardar en buffer, descartar...etc. Esta solución no presenta problemas particulares para las transmisiones UDP ya que se trata de un protocolo no orientado a conexiones. Ahora bien, este mecanismo presenta problemas en TCP ya que no se generan los correspondientes ACK (ACKnowledges) y por lo tanto el rendimiento calculado para esta red híbrida será mucho menor del que tendría en realidad si tuvieramos ACK en el enlace de respaldo. Por estas razones se ha decidido descartar la simulaciones de protocolos TCP por no ser reflejos de la realidad. Nos conformaremos con estudiar los resultados para una conexión CBR sobre UDP. Esta conexión se produce desde el instante 10 hasta el instante 90 entre el nodo 0 y el nodo 1.

Consideramos los mismos indicadores que para el estudio de los protocolos unicast. Para calcular el retardo medio se tendrá en cuenta de forma proporcional el valor del retardo medio para todos los paquetes mandados a través de la VANET y un retardo típico del retardo de aplicaciones de datos UMTS (100 ms). Se considerará además que todos los paquetes que se mandan por UMTS llegan al destino. Esas consideraciones se aproximan a la realidad, por lo tanto las consideramos justificadas.

Debido al hecho de que hemos modificado el protocolo AODV original, es necesario modificar el parse Java que nos permite extraer los resultados de las trazas ns2. Tenemos que contabilizar el número de paquetes que se mandan por el enlace UMTS. Según la proporción del tráfico en cada enlace, calculamos el retardo medio y el porcentaje de éxito de entrega.

### Conexión UDP

Cuadro 5.19: AODV en circuito urbano UDP

| ***Tráfico*** | ***Paq. enviados*** | ***Paq. AODV recibidos*** | ***Pdfr*** | ***Retardo*** | ***Overhead*** |
|---|---|---|---|---|---|
| Alto | 21334 | 8350 | 39,14 | 0,5093 | 418 |
| Medio | 21334 | 9352 | 43,84 | 0,3269 | 396 |
| Bajo | 21334 | 6488 | 30,41 | 0,2128 | 199 |

Cuadro 5.20: Híbrido en circuito urbano UDP

| ***Tráfico*** | ***Paq. enviados*** | ***UMTS*** | ***AODV*** | ***Pdfr*** | ***Retardo*** | ***Overhead*** |
|---|---|---|---|---|---|---|
| Alto | 21334 | 9843 | 1602 | 53,65 | 0,087 | 31 |
| Medio | 21334 | 9919 | 1482 | 53,44 | 0,088 | 35 |
| Bajo | 21334 | 9922 | 1483 | 53,46 | 0,087 | 27 |

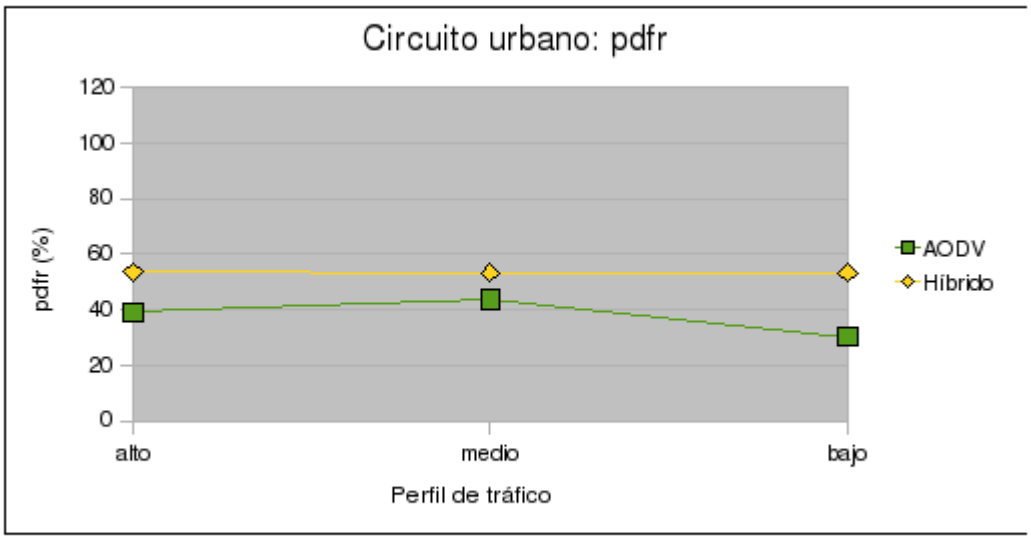



Figura 5.22: Pdfr en circuito urbano

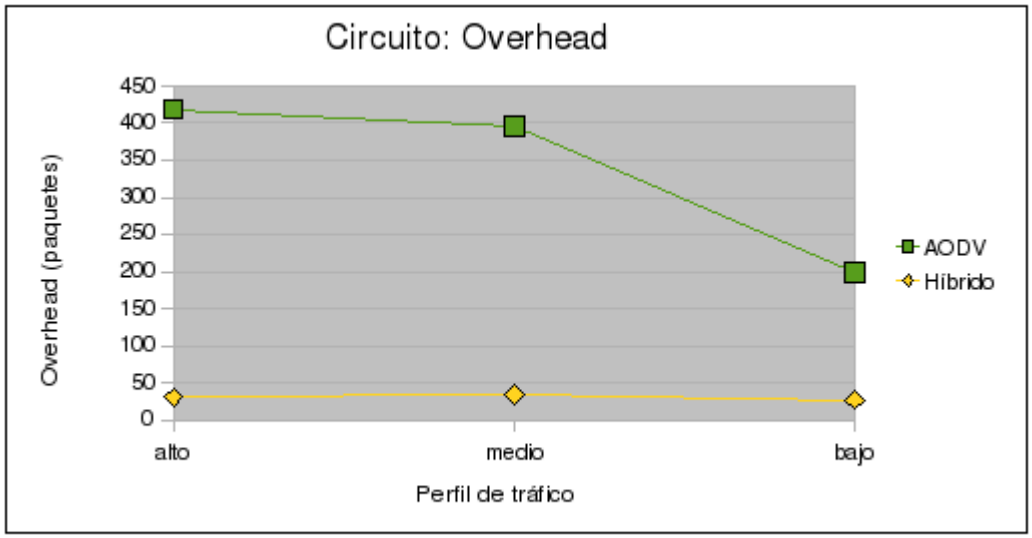



Figura 5.23: Overhead en circuito urbano

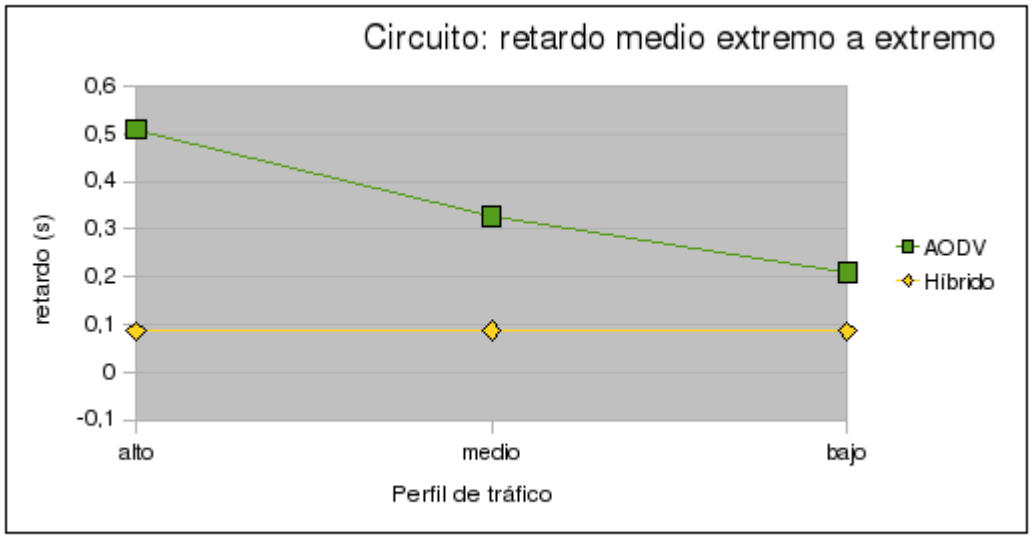



Figura 5.24: Retardo en circuito urbano

De forma general para todos los escenarios de tráfico, vemos que el enlace de respaldo UMTS da estabilidad a la red. Es decir, para todas las densidades obtenemos los mismos rendimientos en cuanto a entrega, retardos y

sobrecarga. La estabilidad introducida es una mejora considerable ya que partiendo de esta estabilidad podremos tener previsiones de tráfico más acertadas, lo cual es una ventaja a la hora de implementar servicios, en particular servicios que requieren calidad de servicio. En todas las gráficas podemos obsevar la casi rectitud de la línea de resultados. Por lo tanto podemos afirmar que introduciendo un respaldo UMTS, hacemos la red VANET más robusta a las variaciones de densidad de tráfico, por consecuencia el protocolo es más adaptado a las redes VANETs que presentan condiciones de movilidad extrememente variables.

El retardo extremo a extremo observado en las redes híbridas es mucho menor que en el caso de VANETs puras. Esto se debe a que la mayor parte de los paquetes generados en la simulación se mandan por UMTS, que presentan retardos menores que las rutas largas de la VANETs.

El overhead también se reduce considerablemente ya que no hay que buscar tantas rutas con tanta frecuencia al descargar el tráfico de la VANET sobre el enlace de respaldo.

### 5.3.2. Comunicaciones en autopista

En este estudio se pretende comparar la plataforma de comunicaciones híbrida: VANET con respaldo UMTS con el protocolo unicast AODV original usando diferentes perfiles de tráfico en autopista. Por ello se considera una conexión CBR sobre UDP ya que hemos subrayado que al no mandar los ACK correspondientes, el protocolo TCP no nos da resultados que reflejan la realidad. La conexión UDP se produce desde el instante 10 hasta el instante 90 entre el nodo 0 y el nodo 2.

Cuadro 5.21: AODV en autopista UDP

| ***Tráfico*** | ***Paq. enviados*** | ***Paq. AODV recibidos*** | ***Pdfr*** | ***Retardo*** | ***Overhead*** |
|---|---|---|---|---|---|
| Alto | 21334 | 7003 | 32,83 | 0,1183 | 1751 |
| Medio | 21334 | 5931 | 25,27 | 0,1700 | 3324 |
| Bajo | 21334 | 10265 | 48,12 | 0,3033 | 1438 |

Cuadro 5.22: Híbrido en autopista UDP

| ***Tráfico*** | ***Paq. enviados*** | ***UMTS*** | ***AODV*** | ***Pdfr*** | ***Retardo*** | ***Overhead*** |
|---|---|---|---|---|---|---|
| Alto | 21334 | 10667 | 10667 | 50 | 0,083 | 42 |
| Medio | 21334 | 9348 | 2637 | 56,18 | 0,079 | 31 |
| Bajo | 21334 | 8512 | 3648 | 57 | 0,0788 | 28 |

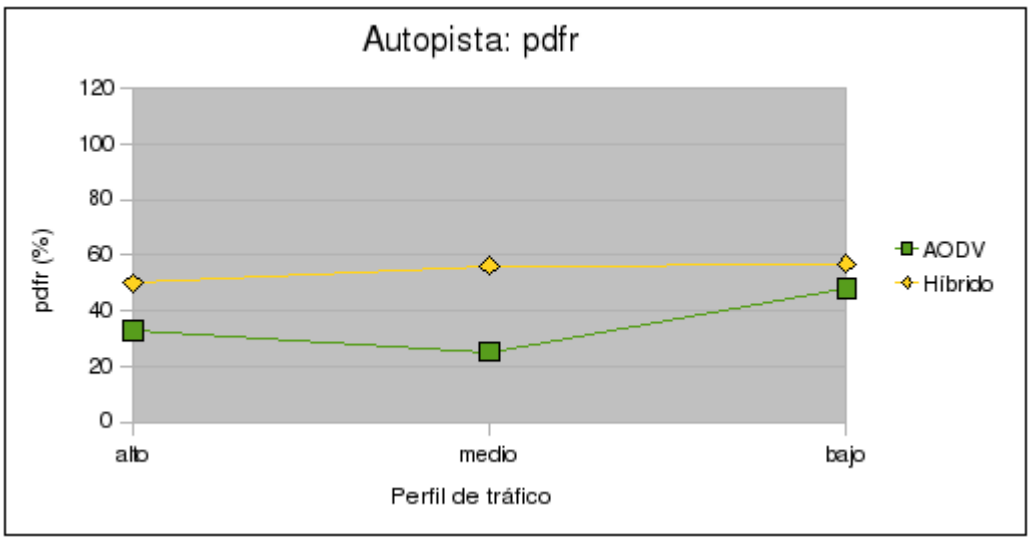



Figura 5.25: Pdfr en autopista

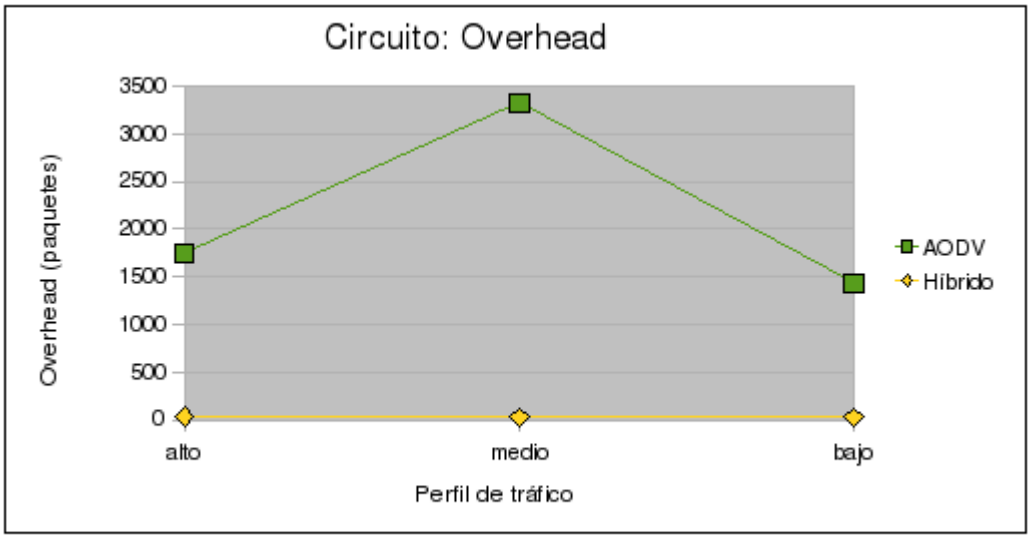



Figura 5.26: Overhead en autopista

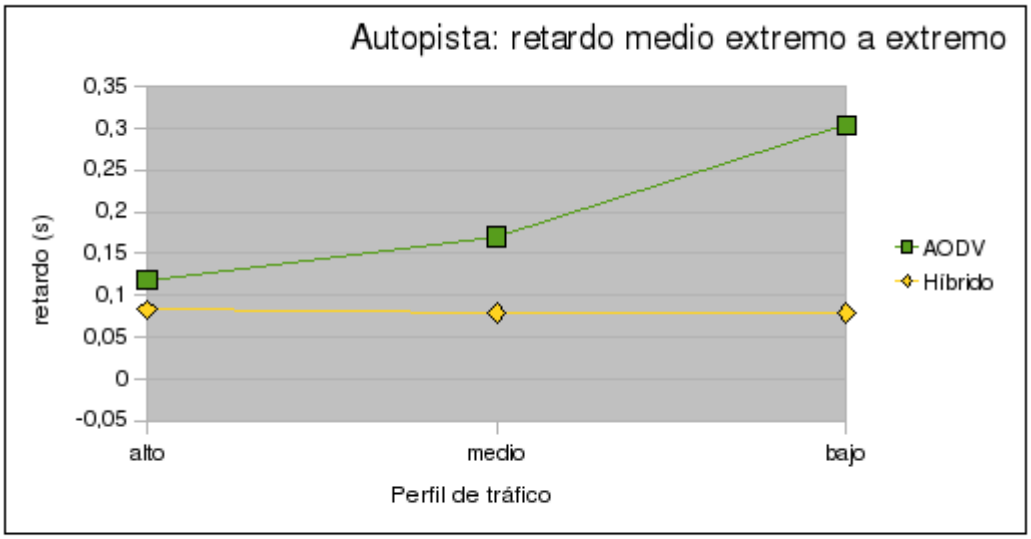



Figura 5.27: Retardo en autopista

Con conexiones UDP en autopista los resultados son identicos a los obtenidos en circuitos UDP. El esquema híbrido es claramente superior en todos

los indicadores, llegando a transmitir más paquetes con menores retardos medios y menos overhead en la red. En autopista, de la misma forma que en circuito, es importante destacar el carácter estable del esquema híbrido, independientemente de los patrones de movilidad del tráfico.

### 5.3.3. Conclusiones generales de la comparativa entre los escenarios de VANET pura y los con respaldo UMTS

La principal conclusión de este capítulo es que, a pesar de las limitaciones en el desarrollo de la solución híbrida se ha conseguido un esquema cuyos rendimientos son bastantes superiores al de una VANET pura sin red de respaldo. El esquema de red híbrida aporta robustez y previsibilidad a la red, lo que es muy útil para gestionar las comunicaciones y así poder preveer la calidad de servicio que se podrá ofrecer en cualquier momento.

En todas las gráficas del estudio se nota que la introdución del enlace de respaldo permite dar resultados constantes independientes del esquema de tráfico, que sea en terminos de entregas, retardos o sobrecargas. Por lo tanto, este esquema de comunicación es muy interesante ya que podremos ofrecer una red estable en situaciones de movilidad distintas.

En todas los escenarios que hemos considerado, se observan tasas de éxito de entregas mayores con retardos y sobrecargas menores. Por lo cual podemos afirmar, que hemos mejorado el rendimiento de la red VANET introduciendo una red de respaldo UMTS.

# Capítulo 6

# Conclusiones

## 6.1. Logros

La principal conclusión obtenida a lo largo de este proyecto es que el despliegue de una plataforma de comunicaciones híbrida en el entorno automóvil puede aportar muchas mejoras a las arquitecturas de comunicaciones inálambricas tradicionales, tanto a Telefónica como a la sociedad en su conjunto.

La plataforma permitirá la implementación de servicios de seguridad vial ayudando el conductor y podiendo contribuir a disminuir la cifras de accidentes en la carretera. Gracias a sistemas de conducción basados en la plataforma de comunicaciones VANET se puede esperar una gestión más eficiente del tráfico basados en servicios de valor añadido paraa los ocupantes de los vehículos. Tales avances son de indudable utilidad para la sociedad en general.

La comparación de protocolos de encaminamiento llevada a cabo en este proyecto nos ha permitido valorar la eficiencia de los protocolos en varios escenarios de comunicación típicos. Hemos obtenido resultados que se podrán reutilizar en otros proyectos.

Uno de los objetivos que nos habíamos propuesto era la definición de una plataforma de simulación para el entorno autómovil. Este objetivo se ha cumplido ya que ahora disponemos de una plataforma de simulación eficiente que nos ha permitido comparar distintos protocolos de comunicaciones. Esa plataforma se podrá reutilizar en otros proyectos y representa un valor añadido al trabajo de Telefónica I+D.

Durante el proyecto hemos sido capaces de identificar los escenarios de comunicación típicos y útiles para el despliegue de servicios en redes VANETs. Además para cada escenario se han definido indicadores de red para medir

el rendimiento de los protocolos. Este logro no debe encasillarse en el marco de este proyecto. Es útil tener una serie de test y de medidas que podremos reutilisar en otras simulaciones o en otras pruebas de terreno.

A nivel de simulaciones de protocolos hemos podido comprobar que las redes VANETs funcionan con rendimientos aceptables, a pesar de los ambientes inestables de muy alta movilidad en los cuales operan. Hemos demostrado que en escenarios de comunicaciones unicast, AODV es claro ganador frente a otros protocolos. En cambio, en escenarios geocast se diferencia entre escenarios de circuito urbanos dónde se demarca LBM y autopistas dónde destaca más un esquema de encaminamiento Geogrid. Hemos sido capaces de demostrar que la introducción de una red de respaldo UMTS a la red VANET mejora considerablemente las prestaciones de las redes VANETs. Esos resultados son fundamentales porque es imprescindible valorar la viabilidad de una solución mediante simulación antes de poder implementar una solución.

Para resumir, el presente trabajo participa en la construcción de un entorno de trabajo riguroso para simular comunicaciones VANETs. Los resultados obtenidos nos confortan en la idea de que sería viable implementar un prototipo de comunicación VANETs. Se han definidos herramientas de trabajo, tales como escenarios e indicadores de red, que definen un marco para futuras simulaciones.

## 6.2. Futuras líneas de trabajo

Obviamente, aunque hemos avanzado en la investigación acerca de las redes vehiculares, queda mucho camino por recorrer y es necesario seguir haciendo esfuerzos investigadores en este campo.

Primero, es necesario seguir investigando para proponer una plataforma de simulación más realista y más completa. Eso pasa por la implementación de nuevos protocolos de encaminamiento dentro del simulador ns2. Tener una implementación propia de un enlace de respaldo UMTS nos daría resultados más aproximados a la realidad y nos permitiría simular también protocolos TCP, generando los ACKs correspondientes. En un futuro es necesario implementar el protocolo AODV con su respaldo UMTS de forma más rigurosa para afinar los resultados presentados en este documento.

Además, sería necesario implementar otros protocolos de encaminamiento, ya que los protocolos basados en información geográfica prometen mejorar de forma significativa los rendimientos en redes VANETs. A partir de mapas, horarios de autobuses, sensores en la carretera, se recoge una información útil

al protocolo de encaminamiento. Una vez implementados esos protocolos en ns2, será necesario volver a realizar una comparativa con los protocolos existentes para comprobar si la información geográfica introduce mejoras en el encaminamiento vehícular.

Otra línea de trabajo interesante sería desarrollar un demostrador para poder realizar pruebas de campo y validar los resultados obtenidos mediante simulación. Las pruebas de terreno son imprescindibles antes de empezar con el desarrollo de una solución ya que las simulaciones, aunque nos dan buenas indicaciones de rendimiento, no son más que una aproximación de la realidad. Por lo tanto, el siguiente paso en nustro trabajo sería desarrollar un nodo de comunicación híbrido AODV/respaldo UMTS para poder comprobar la vialidad de la solución en escenarios reales. El nodo híbrido se deberá empotrar en un sistema embarcado dentro del vehículo. El desarrollo de este demostrados supone un trabajo adicional significativo ya que tendríamos que implementar un protocolo de encaminamiento nuevo y desarrollar los servicios para probar la nueva plataforma de comunicación.

Una alternativa al nodo híbrido de comunicación podría ser un nodo polimorfo. Por polimorfo entendemos un nodo de comunicación donde tendriamos implementados cada uno de los protocolos de encaminamiento que consideramos vencedores en cada uno de los escenarios. A partir de sistemas GPS, mapas de carreteras, sensores para determinar la densidad de tráfico en cada instante, se podría monitorizar el tráfico para determinar en que situación nos encontramos en cada momento. Y a partir de esa información, se cambiaría de un protocolo a otro para utilizar el protocolo lo más óptimo en cada instante. Esa solución, hoy en día no parece muy fiable, debido a la sobrecarga, los retardos de establecimientos de comunicación y l compejidad que conlleva. Sin embargo, la comunidad científica está en continuos avances en estos campos, y pronto podría ofrecernos las garantías de éxito que necesitamos para desarrollar un proceso de encaminamiento polimorfo.

# Apéndice A

# GLOSARIO DE ACRÓNIMOS

**AODV**: Ad-hoc On-Demand Distance-Vector Routing
**BS**: Base Station
**BPSK**: Binary Phase Shift Keying
**CBR**: Constant Bit Rate
**CDS**: Connected Dominating Set
**CSMA/CA**: Carrier Sense Multiple Access With Collision Avoidance
**CTS**: Clear To Send
**DSDV**: Destination Sequenced Distance Vector
**DSR**: Dynamic Source Routing
**DSRC**: Dedicated Short Range Communications
**FSR**: Fisheye State Routing
**FTP**: File Transfer Protocol
**GAMER**: Geocast Adaptative Mesh Environment for Routing
**GPS**: Global Positioning System
**IEEE**: Institute of Electrical and Electronics Engineers
**IP**: Internet Protocol
**ITS** Itelligent Transportation System
**LAR**: Location Aided Routing
**LBM**: Location Based Multicast
**MAC**: Media Access Control
**MANET**: Mobile Ad-hoc Network
**MPR**: Multi Point Relay
**NES**: Neighbor Elimination Scheme
**NFC**: Near Field Communication
**NS2**: network Simulator 2
**OFDM**: Ortogonal Frequency Division Multiplexing
**OLSR**: Optimized Link State Routing
**PDA**: Personal Digital Assistent
**QAM**: Quadrature Amplification Modulation
**QPSK**: Quadrature Phase Shift Keying

**QoS**: Quality of Service
**RIP**: Routing Information Protocol
**RREQ**: Route Request
**RREP**: Route Reply
**RTS**: Request To Send
**SID**: Sistema de Detección de Intrusos
**SUMO**: Simulation for Urban Mobility
**TCP**: Transmission Control protocol
**TORA**: Temporally Ordered Routing Algorithm
**UDP**: User Datagram Protocol
**UMTS**: Universal Mobile Telecommunications System
**UWB**: Ultra Wide Band
**V2V**: Vehicule-to-Vehicule communications
**VANET**: Vehicular Ad-hoc Network
**WAVE**: Wireless Access in the Vehicular Environment
**WPAN**: Wireless Personal Area Network
**ZRP**: Zone Routing Protocol

# Bibliografía

## Enlaces Web


[W1] *Internet Engineering Task Force: MANET Working Group, "Mobile Ad-hoc Networks".* http://www.ietf.org/html.charters/manetcharter.html

[W2] *NAM: Network Animator.* http://www.isi.edu/nsnam/nam/

[W3] *The Network Simulator- NS2.* http://www.isi.edu/nsnam/ns/

[W4] *MObility model generator for VEhicular networks (MOVE)* http://www.csie.ncku.edu.tw/~klan/move/index.htm

[W5] *Simulation of Urban Mobility* http://sumo.sourceforge.net/

[W6] *TraceGraph* http://www.tracegraph.com/

[W7] *Manual del simulador ns2* http://www.isi.edu/nsnam/ns/ns/doc/ns_doc.pdf

[W8] *Marc Greis' Tutorial for ns2* http://www.isi.edu/nsnam/ns/tutorial/index.html

[W9] *Enhanced UMTS Radio Access Network Extensions for ns2* http://www.ti-wmc.nl/eurane/


## Textos


[CEPERSD 2003] Charles E. Perkins, E. Royer, S.Das *Ad-hoc On-Demand Distance-Vector Routing Algorithm for Mobile Wireless Networks*,RFC 3561, Julio 2003.

[CEPPB 1994] Charles E. Perkings, Pravin Bhagwat, *Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers*, 1994.

[DBJDAMJB 2004] David B Johnson, David A. Maltz, Josh Broch. *DSR: the Dynamic Source Routing protocol for multihop wireless ad-hoc networks.* Computer Science Department, Carnegie Mellon University, Pittsburg, 2004.

[DBJDAMYH 2004] David B Johnson, David A. Maltz, Yih-Chun Hu. *The Dynamic Source Routing Protocol for Mobile Ad-hoc Networks (DSR).* Internet Draft. Julio 2004

[FIDSIS 2005] François Ingelrest, David Simplot-Ryl, Ivan Stojmenović. *Broadcasting in Hybrid Ad-Hoc Networks.* 2005

[JBMDATXC 2004] Jeremy Blum, Min Ding, Andrew Thaeler, Xiuzhen Cheng. *Connected Dominating Set in Sensor Networks ans MANETs.*Department of Computer Science The George Washington University, Washington. 2004

[MGXH 2002] Mario Gerla, Xiaoyan Hong, *Fisheye State Routing Protocol (FSR) for Ad-Hoc Networks*, Dratf IETF, Junio 2002.

[NB 2008] Nicklas Baijar, *Zone Routing Protocol (ZRP)*, Networking Laboratory, Helsinki University of Technology, 2008.

[OKRG 2002] O. Kachiriski, R. Guha , *Intrusion detection using mobile agents in wireless ad-hoc networks*, IEEE WorkShop, 2002.

[PYEKTC 2004] Peiling Yao, Eg Krhone, Tracy Camp. *Evaluation of Three Geocasting Protocols for a MANET*, Dept. of Math and Computer Sciences, Colorado School of Mines, 2004.

[RSCALF 2005] Roberto Subiela Durá, Dr.Antonio León Fernández. *Simulación de protocolos de encaminamiento en redes móviles ad-hoc con NS-2*, Universidad Politécnica de Valencia, ,2005.

[SLYK 2006] Sung-Hee Lee, Youg-Bae Ko. *An efficient Neighbor Knowledge Based Broadcasting for Mobile Ad-Hoc Networks.* College of Information and Communication,Ajou University, Suwon, South Korea. 2006

[SYRK 2004] Seung Yi, Robin Kravets, *Composite Key Management for Ad-hoc Networks*, Dept of Computer Science, University of Illinois, 2004

[TCPJ 2003] T.Clausen, P. Jacquet . *Optimized Link State Routing Protocol (OLSR)*, RFC 3626, Octubre 2003.

[WLYTKLJS 2000] W, Liao,Y. Tseng, K.Lo, J.Shen. *GeoGrid: A Geocasting protocol for mobile ad-hoc networks based on GRID.* Journal of Internet Technology, 2000.

[YKNHV 1998] Young-Bae Ko, Nitin H. Vaidya, *Location-Aided Routing (LAR) in mobile ad hoc networks*, Department of Computer Science, Texas AM University, 1998.

[YKNHV 1999] Young-Bae Ko, Nitin H. Vaidya. *Geocasting in Mobile Ad Hoc Networks: Location-Based Multicast Algorithms*, Department of Computer Science, Texas AM University, 1999.

[YZWL 2000] Y. Zhang, W. Lee *Intrusion detection in wireless ad-hoc networks*,2000.

[ZHMPPS 2002] Zygmunt Haas, Marc Pearlman, Prince Samar. *The Zone Routing Protocol (ZRP) for ad-hoc networks*, INTERNET-Draft, Julio 2002.